TrusCont
Trusted Content Delivery

TrusCont Ltd | 87 Moshe Goshen Ave, 2nd Floor, Qiriat Motzkin 26313, Israel | Tel: +972 4 832 0555 Fax: +972 4 832 0550

TrusCont™

TSFD Protection Toolkit

Version 2.4

User's Manual

September 2011

© 2006-2011 TrusCont Ltd.

Table of Contents

1. INTRODUCTION 8

1.1 TSFD KEY FEATURES 8

1.2 WHAT'S NEW IN VERSION 2.4 8

1.3 WHAT'S NEW IN VERSION 2.3 9

2. BEHAVIOR OF PROTECTED CONTENT 11

2.1 SOFTWARE PROTECTION 11

2.2 CONTENT PROTECTION 15

2.2.1 Operating Systems Compatibility for Running Protected Content Files 24

2.3 PROTECTION OF SOFTWARE, AND CONTENT FILES ON THE SAME DISK 25

2.4 LOCAL ADMINISTRATOR RIGHTS 25

3. CHOOSING PROTECTION STRATEGY 26

4. INSTALLING TRUSCONT TSFD PROTECTION TOOLKIT 27

4.1 SYSTEM REQUIREMENTS 27

4.2 STARTING THE INSTALLATION 27

5. USING TRUSCONT TSFD PROTECTION TOOLKIT 28

5.1 OVERVIEW 28

5.2 CREATING A NEW PROJECT 28

5.2.1 Preparing Your Content 28

5.2.2 Starting a New Project 29

5.2.3 Editing a Project 30

5.2.3.1 Adding Files and Folders 32

5.2.3.2 Removing Files and Folders 34

5.2.3.3 Marking Files for Protection 34

5.2.3.4 Protecting Digitally Signed Program Files 34

5.2.3.5 Customizing Copy Protection Options for Individual Program Files 34

5.2.3.6 Customizing Copy Protection Options for Individual Content Files 36

5.2.3.7 Copy Protection Options by File Type 38

5.2.3.8 Customizing Copy Protection Options for Multiple Files 39

5.2.3.9 Clearing a Project 39

5.2.4 Changing Advanced Project Settings 39

5.2.4.1 Setting a Global Password 40

5.2.4.2 Forcing Time Limit Verification Using External Time Source Only 41

5.2.4.3 Enabling and Disabling Content Protection Notifications 41
5.2.4.4 TrusCont Autorun File Name 42
5.2.4.5 Viewing the List of 3rd Party Applications 43
5.2.4.6 Restricting Use of TSFD to Specific Number of Computers, Users, or a Domain 43
5.2.5 Naming a Project 45
5.2.6 Saving & Duplicating Your Project 45
5.2.7 Creating a Portable Image (.tcpi) 47*
5.2.8 Creating a Portable Image (.exe) 49*
5.3 MODIFYING SAVED PROJECTS 50
5.4 OPENING EXISTING PROJECTS FOR DUPLICATION 50
5.4.1 Selecting the Target TSFD device 50
5.4.2 Duplicating on Multiple Devices 51
5.4.3 Partitions Configuration 51
5.4.3.1 CD-ROM Emulation & Autorun Support 52
5.4.3.2 Read Only Partitions 52
5.4.3.3 Read Write Partitions 52
5.4.3.4 Possible Partitions Configurations 53
5.4.4 Setting a Publisher Password 53
5.4.5 Confirming Overwrite and Starting the Duplication 53
5.5 USING THE TOOLKIT'S PROJECT FILE ASSOCIATION 55

6. ADVANCED LICENSING AND PUBLISHING OPTIONS 56

6.1 CREATING A CUSTOM LICENSE TYPE 56
6.1.1 Entering the License Management System 56
6.1.2 Checking Account Balance 57
6.1.3 Creating a New License Type 59
6.1.4 Allocating Additional Custom Licenses 61

7. LICENSING PRODUCTION TO SERVICE PROVIDERS 63

7.1 CREATING AN IMAGE THAT REQUIRES A CUSTOM LICENSE 63
7.2 TRANSFERRING CUSTOM LICENSES TO A SERVICE PROVIDER 64

8. UPDATING CONTENT ON TRUSCONT SECURE FLASH DRIVES 66

8.1 MAKING A PRODUCT UPDATEABLE 66
8.2 CREATING TSFD UPDATES 66
8.3 CREATING AN UPDATE FILE 67
8.3.1 Creating Generic Updates 68
8.3.2 Creating Updates for TSFDs Containing a Specific Product 70
8.3.3 Updates that require a license 71

8.3.3.1 Creating a Custom License Type 71
8.3.3.2 Creating the Image 72
8.3.3.3 Generating License Code for End Users 72
8.3.3.4 Creating Multiple Updates for the Same Product 75
8.3.4 Updates that Create a New Product 76
8.4 ADDING A WELCOME PAGE AND A LICENSE AGREEMENT 78
8.5 APPLYING AN UPDATE 79
9. TROUBLESHOOTING & KNOWN ISSUES 82
APPENDIX A – CUSTOMIZING 3RD PARTY APPLICATIONS SUPPORT FOR CONTENT PROTECTION 86
APPENDIX B – TSFD LICENSE REQUIREMENTS BY FEATURES 89
APPENDIX C – THE TSFD LICENSE TERM 90
APPENDIX D – TRUSCONT CONTENT PUBLISHING SERVER 91

Table of Figures

Figure 1: Running a Protected Application 11
Figure 2: Running a Protected Application without the Original TSFD 12
Figure 3: Protecting Program Files with a Password 13
Figure 4: Limiting Applications with Expiration Dates 14
Figure 5: Limit Use to Specific Number of Computers, User, or a Domain 14
Figure 6: The TrusCont Autorun File 16
Figure 7: Copy & Paste Restriction Notification 18
Figure 8: Printing Restriction Notification 18
Figure 9: File save notification 19
Figure 10: Password Protection for Content Files 20
Figure 11: Global Password Dialog 21
Figure 12: Notification on Expiration Date of a Protected Content File 21
Figure 13: TSFD Disconnect Notification 23
Figure 14: Opening Protected Files with Unsupported Applications 24
Figure 15: The Welcome Page 29
Figure 16: Select Task Page 30
Figure 17: The Edit Project Page 31
Figure 18: Tabs in the Edit Project Page 32
Figure 19: Add Folder Dialog 33
Figure 20: Add Files Dialog 33
Figure 21: Copy Protection Options for Individual Program Files 36
Figure 22: Copy Protection Options for MP3 Music Files 37
Figure 23: Copy Protection Options for PDF Documents 37
Figure 24: Setting Protection Options for Multiple Files 39
Figure 25: Advanced Project Settings 40
Figure 26: Setting a Global Password 40
Figure 27: Enabling and Disabling Content Protection Notifications 41
Figure 28: Changing TrusCont Autorun File Name 42

Figure 29: Customizing the List of Allowed Applications 43
Figure 30: Setting Advanced Use Restrictions 44
Figure 31: Volume Information Page 45
Figure 32: Saving and Duplicating New Projects 46
Figure 33: Save Project Page 47
Figure 34: Advanced Publishing & Licensing Options Page 48
Figure 35: Creating a Portable Image 49
Figure 36: Select Target Page 50
Figure 37: Partitions Configuration & Publisher Password Page 51
Figure 38: Overwrite Warning Page 54
Figure 39: TSFD Recording Process 55
Figure 40: License Management System Login Page 57
Figure 41: Home Page of the License Management System 58
Figure 42: List of License Accounts 58
Figure 43: Account Balance 59
Figure 44: Creating a New License Type 60
Figure 45: List of Custom License Types 60
Figure 46: Checking the Balance of Custom License Types 61
Figure 47: Allocate Additional Custom Licenses 62
Figure 48: Crating an Image that Requires a Custom License Type 64
Figure 49: Transferring Custom Licenses to a Service Provider 65
Figure 50: Creating an Update File 68
Figure 51: Creating Generic Updates 69
Figure 52: Creating an Update for TSFDs Containing a Specific Product 70
Figure 53: Account Balance with Multiple Custom License Types 71
Figure 54: Creating an Update that Requires a License 72
Figure 55: Creating a License Code 73
Figure 56: The 'Create License Code' Form 74
Figure 57: License Codes List 75
Figure 58: License Types Balance 76
Figure 59: Creating an Update that Create a New Product 77
Figure 60: Adding a Welcome Page and a License Agreement 78

Figure 61: Sample Welcome Page 79
Figure 62: End User License Agreement Sample 80
Figure 63: Target Drive and License Code 81
Figure 64: The Update Recording Process 81
Figure 65: Previously Protected Files Indication 82
Figure 66: Unsupported Files Indication 83
Figure 67: Unsupported Files Notification 84
Figure 68: Certified Application List 86
Figure 69: The Application Setup Form 87
Figure 70: TrusCont Content Publishing Server 91

1. Introduction

Thank you for choosing TrusCont security solutions. TrusCont products are specifically designed for secure distribution and delivery of digital contents.

TrusCont Secure Flash Drive (TSFD) is a sophisticated USB flash drive that contains built in security enhancements such as copy protection. Unlike standard USB flash drives, the TSFD includes a powerful internal microcontroller, which is programmed to secure the content stored on it.

TSFD is a powerful hardware based copy protection solution for securing software, documents, multimedia files, and other digital content. One of the major advantages the TSFD has comparing to traditional dongles is its huge memory capacity, ranging from 1GB to 32GB. This allows publishers to distribute their product on the TSFD itself, together with any accompanying such as documentations, and video guides.

1.1 TSFD Key Features

- Powerful hardware based copy protection for Software (32bit program).
- Copy protection for documents, pictures, music files, video clips, and other content files.
- Printing and Copy & paste control.
- Time limits – make your files expire at a specific date.
- Limit use of the TSFD to specific number of computers, or users.
- Limit use of the TSFD to a specific domain.
- Password protection.
- Huge storage capacity (up to 32 GB).
- Read only option, CD-ROM Emulation – prevent erase, enable true Autorun.
- Easy to use duplication software – TrusCont TSFD Protection Toolkit.

1.2 What's New in Version 2.4

- **Preliminary Support for Windows 8 Developers Preview Edition**

  Most file types that can be protected with version 2.4 of the TSFD Protection Toolkit will play on Windows 8 Developers Preview Editions.

  Important note: Windows 8 is still under development and is subject to changes. There is no guaranty that files protected with version 2.4 of the Toolkit will play properly on Windows 8 (both existing and future editions).

- **Support for New Flash Chips**

  The TSFD Protection Toolkit supports new USB Flash Drive controllers, and flash chips technologies that have emerged in recent year. Some of these technologies are embedded in new TSFD models that are incompatible with earlier version of the Toolkit.

1.3 What's New in Version 2.3

- **New DRM Features**

  Limit use of TSFDs to specific number of computers, users, or a domain.

- **Internet Publishing**

  Compile a data set to a single EXE file that automatically installs itself to your customers' TSFDs and TSFD Ready flash drives.

- **TSFD Updates**

  Publish updates to TSFDs that were already sent to end users. Updates can be made available to specific products, specific customers, or all customers.

- **Support for Windows 7**

  TrusCont TSFD Protection Toolkit now officially supports Windows 7. The product was tested to make sure full compatibility with the new operating system.

- **Product no longer requires Ahead Nero**

  Product now uses TrusCont proprietary engine and Windows components. Customers are no longer required to purchase 3rd party applications for using the Toolkit.

- **Content Protection – Support for 3rd party applications**

  The Toolkit now automatically allows all 3rd party applications on the TSFD to read protected content files. This allows customers to protect content files for use in custom applications located on the disc. This option is enabled by default and can be disabled in the Project Edit page.

- **Support for proprietary file formats**

  Customers can now protect file formats that are not supported by the Toolkit by default. This feature can also be used to protect proprietary file formats.

- **New Time Limit Option – Use external time source only**

  A new feature allowing publishers to set stronger time limits by forcing verification using only external time source. This option results in a stronger time limit but requires internet connection in order for the protected application to run.

2. Behavior of Protected Content

This section describes how your content will behave once protected and recorded on TSFD devices. The behavior depends on your content type. This section describes the behavior of protected software, and the behavior of protected content files (documents, video clips and other file types that are not program files).

2.1 Software Protection

The copy protection for software program files is fully transparent to the end users as long as the TSFD on which it was recorded is connected to the host computer. The protected program file runs and functions normally just as its unprotected origin. The images below show an example of running a protected application by double clicking it in Windows Explorer.

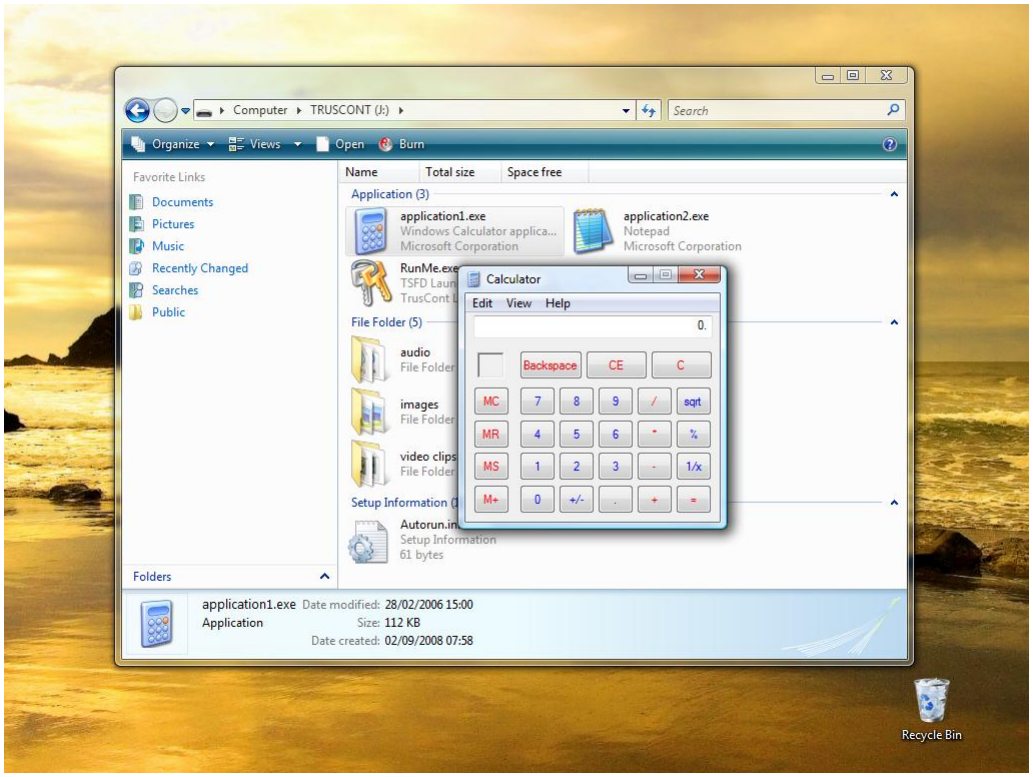

Figure 1: Running a Protected Application

Anti-Copy Protection

The copy protection system embedded within the protected file transparently verifies that the original TSFD is connected to the host computer and then allows the file to run. If the original TSFD is not connected to the host computer, a message requesting the end user to connect the original USB disk is displayed.

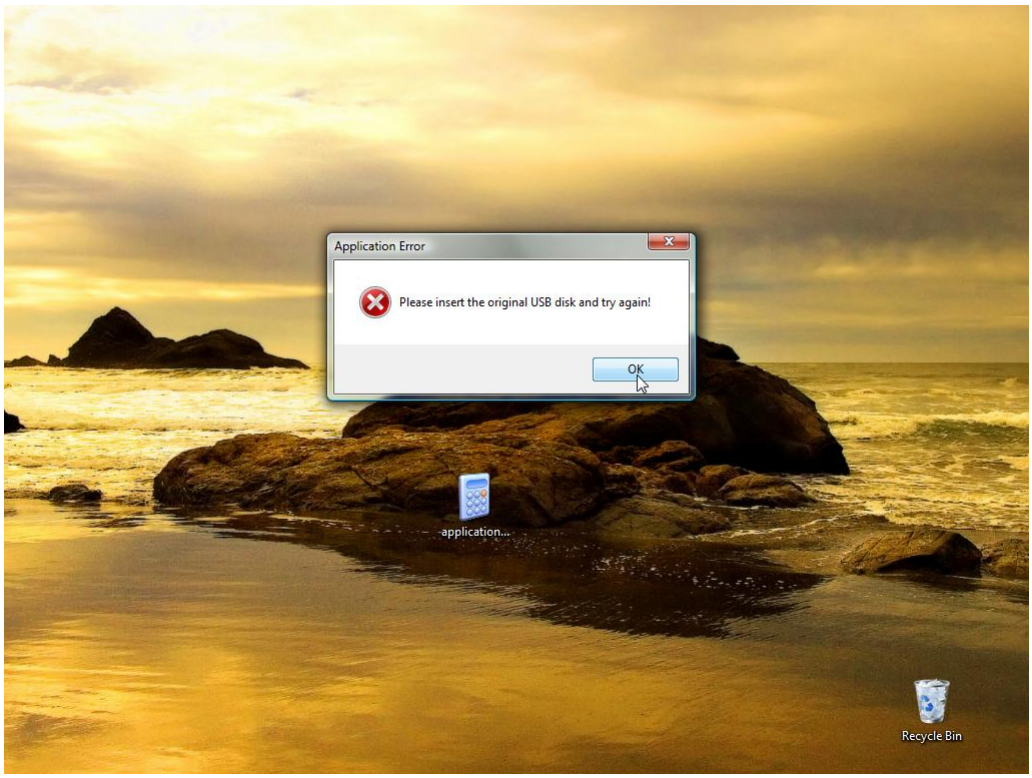

Figure 2: Running a Protected Application without the Original TSFD

Password protection

Optionally, program files can be protected also with a password. If a password is set, the copy protection system will also ask the end user for a password immediately after verifying that the original TSFD is connected to the host computer. If the password is correct the application will run. Otherwise an error message will appear. A TSFD can contain numerous protected files. Each file may have a different password.

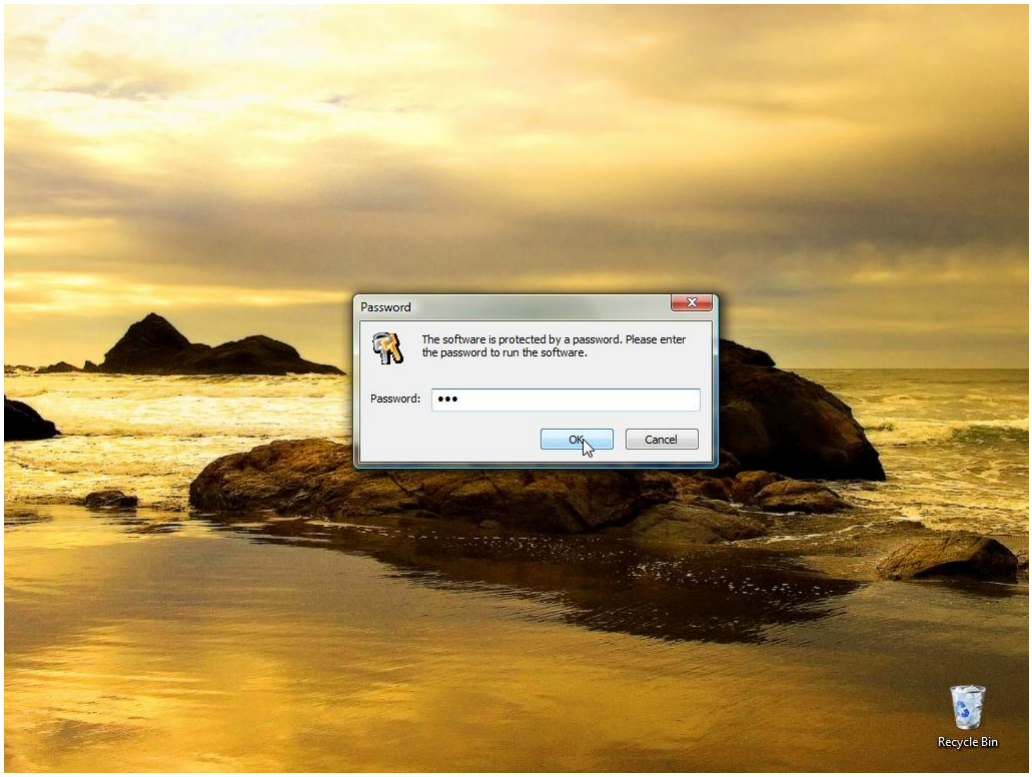

Figure 3: Protecting Program Files with a Password

Expiration Dates

Another protection layer that can be applied to program files is expiration date. Expiration dates are useful to make sure your customers are not using outdated software. Trying to run a protected file after the expiration date will display an error message indicating the file has expired. A TSFD may contain numerous protected files. Each file may have a different expiration date.

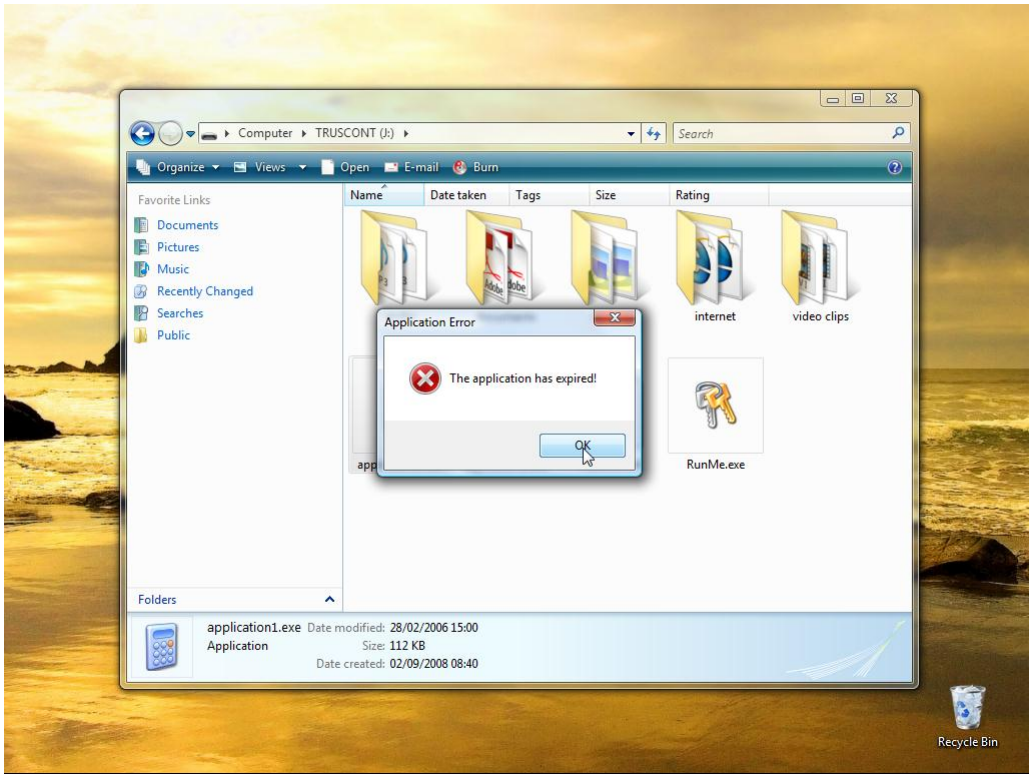

Figure 4: Limiting Applications with Expiration Dates

Limit use to specific number of computers, users, or a domain

You can restrict the use of the TSFD to a specific number of computers. If the TSFD is restricted for 3 computers it means it will run normally on the first 3 computers but when trying to run it on a fourth computer the following message will appear.

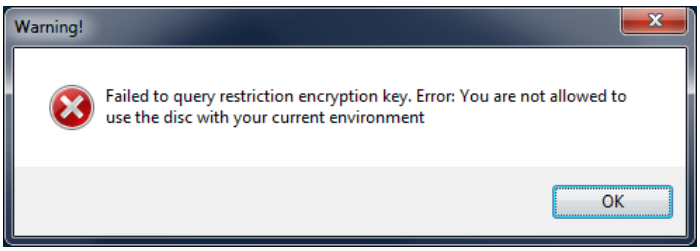
Warning!
Failed to query restriction encryption key. Error: You are not allowed to use the disc with your current environment
OK

Figure 5: Limit Use to Specific Number of Computers, User, or a Domain

Restricting use of a TSFD to computers, users or a domain requires the end users to have internet connection for the first use of the TSFD on each computer.

You can restrict the use of the TSFD also to a specific number of users. In this case the TSFD can be used on many computers but only with the same Windows user. This works well on networks with a domain controller. The same domain user can login to different computers and use a

TSFD that was restricted for 1 user. But a second user cannot use the TSFD even if he logs in to the same computers.
Note: Users with the same login name are not the same user.

The third restriction option is restricting to a network domain. This means all the computers and users of the network domain will be able to use the TSFD. The TSFD is locked to the domain on which it is first used. This option is useful for restricting use of TSFDs to a specific network, office, or organization.

Important note: A protected TSFD can be used only on one computer at the same time regardless of the restriction settings. In order to use a TSFD on a specific computer the TSFD must be connected to a USB port of the computer.

2.2 Content Protection

Behavior of content files is different from the behavior of program files. The main reason for the differences is that content files are not independent files. Pictures, music files and video clips for example require a 3rd party viewing/playing application such as Internet Explorer, and Windows Media Player.

When protecting content files, the TSFD Protection Toolkit automatically adds a small Autorun file to your TSFD. The default name of the TrusCont Autorun file is "RunMe.exe". This file loads the TrusCont security software modules that allow 3rd party applications to read the protected content files transparently, and most important – in a secure manner.

The TrusCont Autorun file doesn't affect the original Autorun functionality of your files. After the runme.exe file is loaded into memory it automatically runs the original Autorun file(s) you may have on your project.

When the TrusCont Autorun file loads it looks for the original TSFD on which it was recorded. If the TSFD is connected to the computer it grants access to the protected content. Otherwise, the protected files remain unusable.

Once the TrusCont Autorun is loaded, the protected content files can be viewed / played normally just as their unprotected versions, with one limitation – only applications certified by TrusCont and listed in the certified applications list of the Toolkit (see section *5.2.4.5*

Viewing the List of 3rd Party Applications) can be used to view/play protected files. However, it is possible to customize the list of certified applications and even add support for proprietary applications (see *Appendix A – Customizing 3rd Party Applications Support for Content Protection*).

Although the protected files can be viewed normally in common applications such as Adobe Acrobat Reader, or Microsoft Internet Explorer, it is impossible to copy their content utilizing 'Save As', 'Copy & Paste', Printing and other common techniques, based on the specific restrictions set by the publisher that has originally recorded the content.

Note: If your project already contains a file with the name Runme.exe, you can rename of the TrusCont Autorun file. See section *5.2.4.4 TrusCont Autorun File Name*.

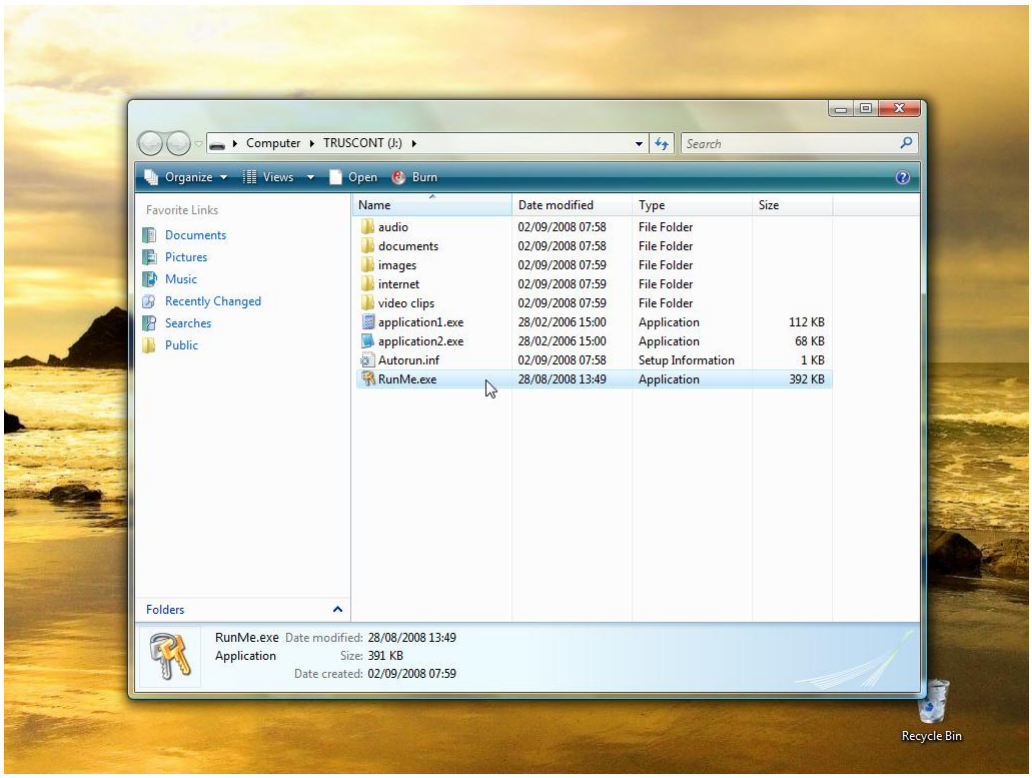

Figure 6: The TrusCont Autorun File

When an end user tries to perform an operation that violates the security policy set by the publisher, a notification window appears, explaining the end user that the operation he tries to perform is not permitted. These notifications are displayed in a Windows Vista style, where the entire desktop is darkened and the notification appears in a bright centered window.

The following images show examples for notifications displayed when an end user tries to perform various operations on an HTML document protected by the strictest policy:

A. Copy & Paste

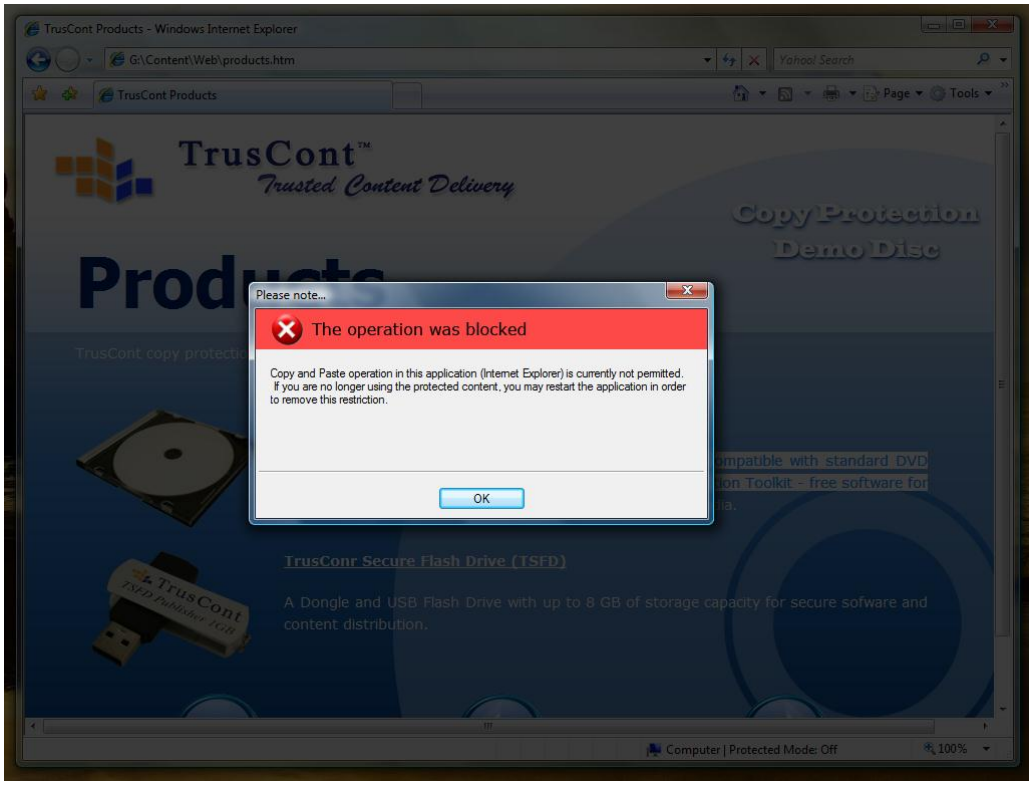
TrusCont Products - Windows Internet Explorer
G:\Content\Web\products.htm
TrusCont Products
TrusCont™
Trusted Content Delivery
Copy Protection
Demo Disc
Please note...
The operation was blocked
Copy and Paste operation in this application (Internet Explorer) is currently not permitted.
If you are no longer using the protected content, you may restart the application in order to remove this restriction.
OK
TrusConr Secure Flash Drive (TSFD)
A Dongle and USB Flash Drive with up to 8 GB of storage capacity for secure sofware and content distribution.
Computer | Protected Mode: Off
100%

Figure 7: Copy & Paste Restriction Notification

B. Printing

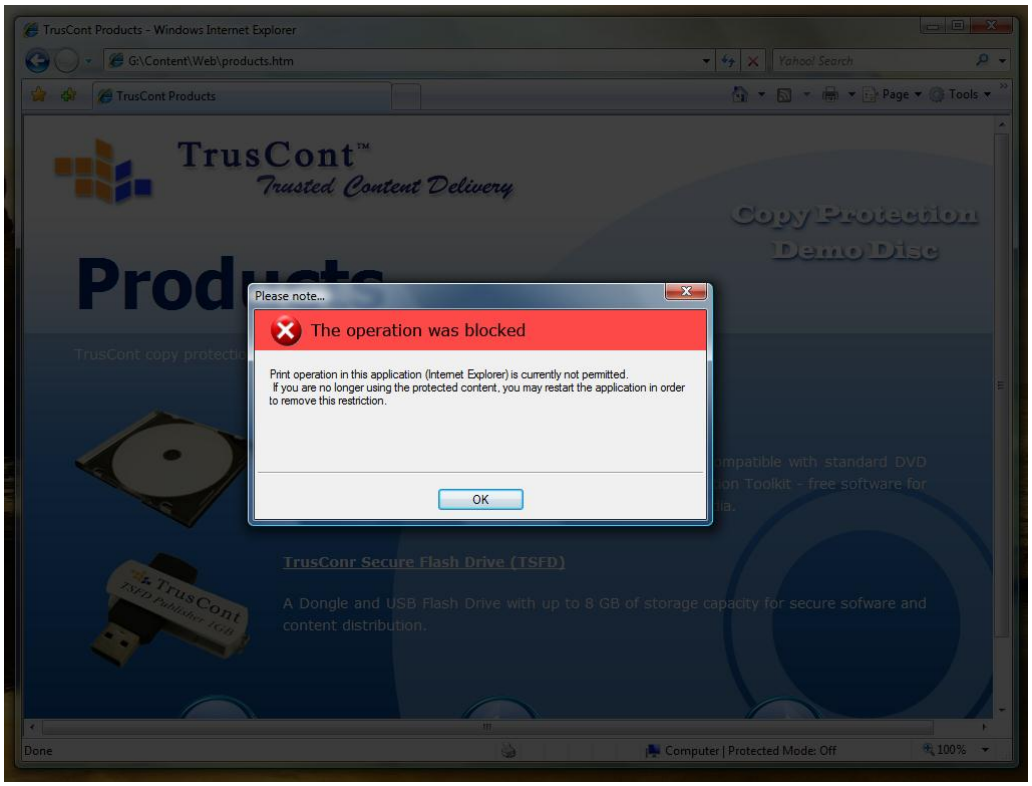
TrusCont Products - Windows Internet Explorer
G:\Content\Web\products.htm
TrusCont Products
TrusCont™
Trusted Content Delivery
Copy Protection
Demo Disc
Please note...
The operation was blocked
Print operation in this application (Internet Explorer) is currently not permitted.
If you are no longer using the protected content, you may restart the application in order to remove this restriction.
OK
TrusConr Secure Flash Drive (TSFD)
A Dongle and USB Flash Drive with up to 8 GB of storage capacity for secure sofware and content distribution.
Done
Computer | Protected Mode: Off
100%

Figure 8: Printing Restriction Notification

For security reasons, an application displaying protected content automatically inherits the restricted behavior of the protected files opened by it. This means the restrictions will apply also to other files that are opened / displayed in the specific application until the specific application is closed and restarted without further opening any protected files.

Different protected files can have different restrictions, even if they are stored on the same TSFD. For example, on one document 'Copy & Paste' may be restricted and 'Printing' allowed, while on a second document 'Printing' may be restricted and 'Copy & Paste' allowed. An application displaying multiple protected files will always inherit the most strict security policy. In this case, both 'Printing' and 'Copy & Paste' will be restricted on both documents.

C. 'Save', 'Save As', and Other File Saving Options

Unlike 'Copy & Paste' and 'Printing', saving protected files to the hard drive or any other medium is always restricted and cannot be configured even by the publisher of the content. This includes also files and programs downloaded using Internet browsers while protected files are in use. When a user tries to save a protected file a dialog box appears, notifying the user that any files he saves will become invalid as soon as the application is closed. The user has the option of allowing the file save operation anyway or blocking it. If the user chooses to save the file anyway the file will be temporary available until the user closes the application.

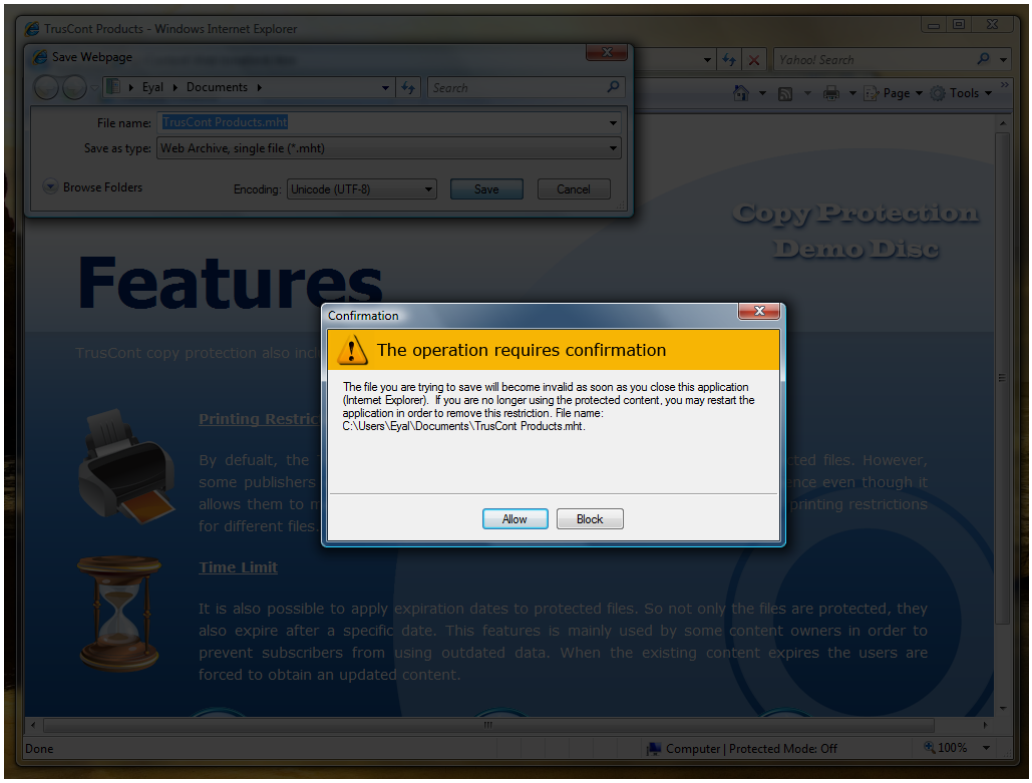
TrusCont Products - Windows Internet Explorer
Save Webpage
File name: TrusCont Products.mht
Save as type: Web Archive, single file (*.mht)
Browse Folders
Encoding: Unicode (UTF-8)
Save
Cancel
Copy Protection Demo Disc
Features
Confirmation
The operation requires confirmation
The file you are trying to save will become invalid as soon as you close this application (Internet Explorer). If you are no longer using the protected content, you may restart the application in order to remove this restriction. File name: C:\Users\Eyal\Documents\TrusCont Products.mht.
Allow
Block
Time Limit
Done
Computer | Protected Mode: Off
100%

Figure 9: File save notification

On-Access Passwords

Content files can also be protected with a password similar to the password protection of program files. When opening a protected file, such as a document or a movie clip for example, the copy protection system displays a dialog box requesting a password. If the password is correct the file opens. Otherwise, the content of the file is unavailable. A TSFD may contain numerous protected files. Each file may have a different password.

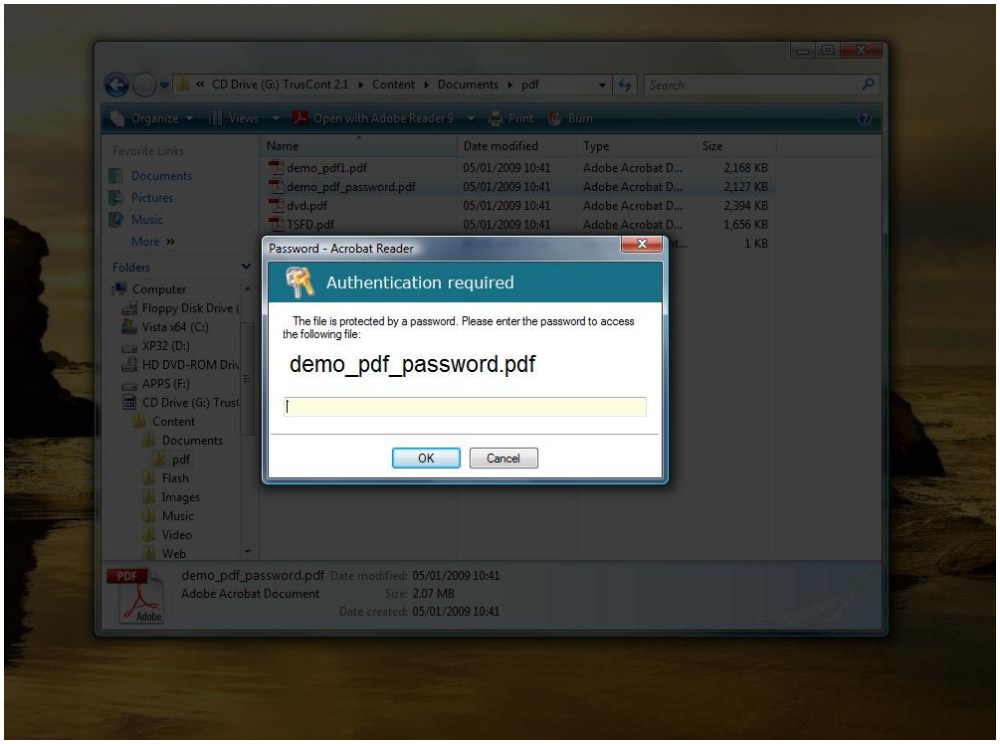
Password - Acrobat Reader
Authentication required
The file is protected by a password. Please enter the password to access the following file:
demo_pdf_password.pdf
OK
Cancel

Figure 10: Password Protection for Content Files

Global Passwords

In addition to setting a password to each individual file, it is also possible to set a global password for the entire TSFD. If a TSFD is protected by a global password, a dialog box asking for the global password appears upon connection of the TSFD to the host computer.

Global passwords secure only protected content files. If the end user enters the correct password, access is granted to all the files stored on the TSFD (provided that they are stored on the original TSFD on which they were originally recorded). If the end user fails to provide the correct password, access to the protected content files is denied. However, access to protected program files, and other unprotected files that may be stored on the same TSFD is not affected.

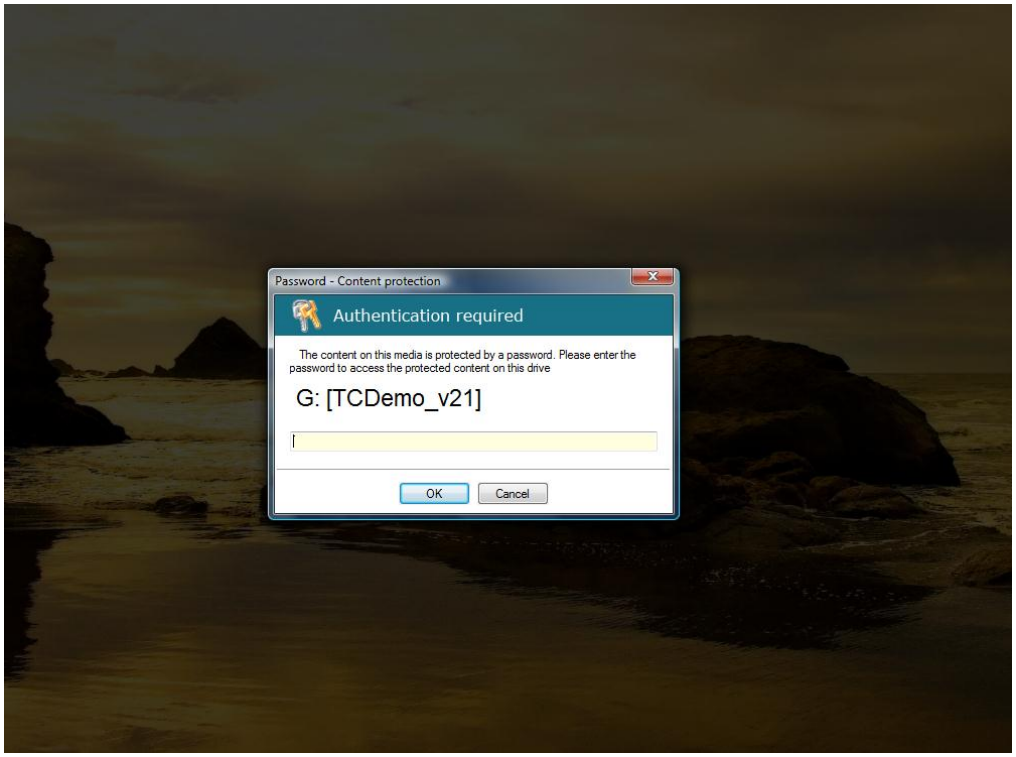
Password - Content protection
Authentication required
The content on this media is protected by a password. Please enter the password to access the protected content on this drive
G: [TCDemo_v21]
OK
Cancel

Figure 11: Global Password Dialog

Expiration Dates

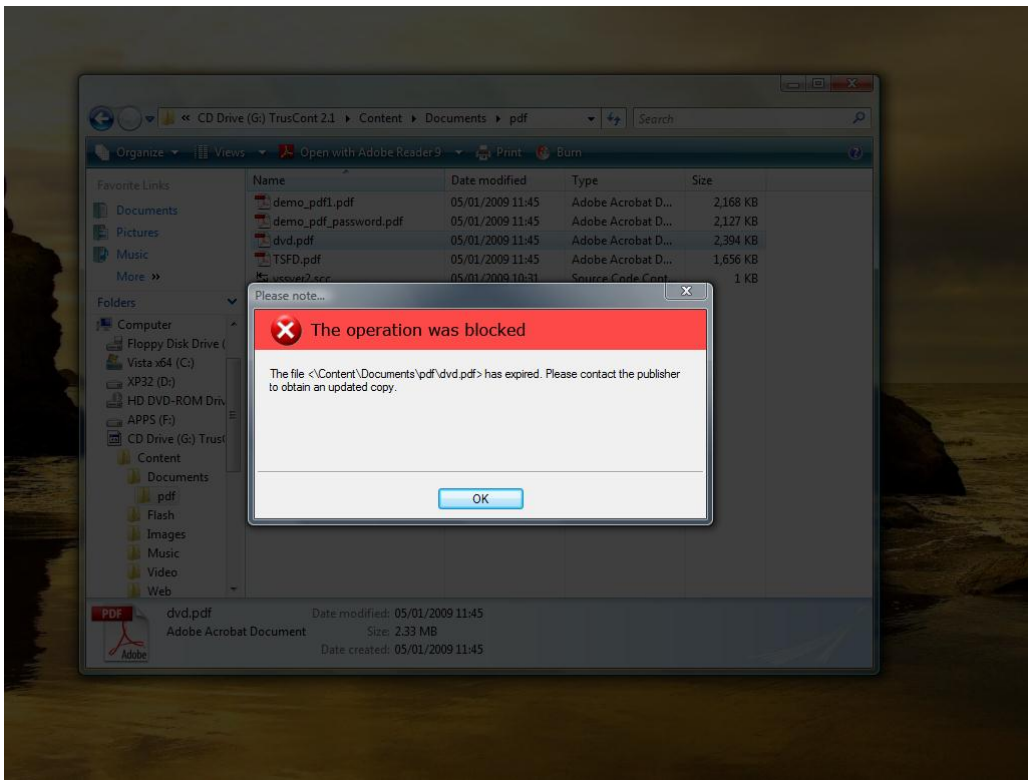

Figure 12: Notification on Expiration Date of a Protected Content File

Another protection layer that can be applied to content files is an expiration date. Expiration dates are extremely useful to make sure your customers are using the most relevant and up-to-date documents. For example, publishers of service manuals, schematics, procedures and other types of documents can make sure that their field engineers use documents that correspond to the recent systems, spare parts, schematics, etc. after the expiration date will trigger an error message indicating the file has expired. A TSFD may contain numerous protected files. Each file may have a different expiration date.

Limit use to specific number of computers, users, or a domain

Restricting a TSFD to specific number of computers, users or a domain will actually apply the restriction on all program files including the TrusCont Autorun file that grants access to protected content files. If the TrusCont Runme.exe file is allowed to run on the specific computer / user / domain access to the protected content files will be granted. Otherwise the Runme.exe will not load and access to the protected files will be denied.

Disconnecting the TSFD While Protected Content is in Use

3rd Party applications that read protected files automatically inherit their security policy. This means that operations such as 'Copy & Paste' and 'Printing' may be applied to any other files opened within the same applications, even if these files are not protected at all. Restarting the applications without further opening any protected files removes these restrictions.

If applications that accessed protected content are still open when the TSFD is disconnected from the host computer, the copy protection system displays a notification specifying which applications are still working in restricted mode. These are the applications that need to be restarted in order to return to their natural operation mode.

Please note that protected content files can be viewed / played only directly from the TSFD. This means that the TSFD must be connected to the host computer as long as the protected files are in use.

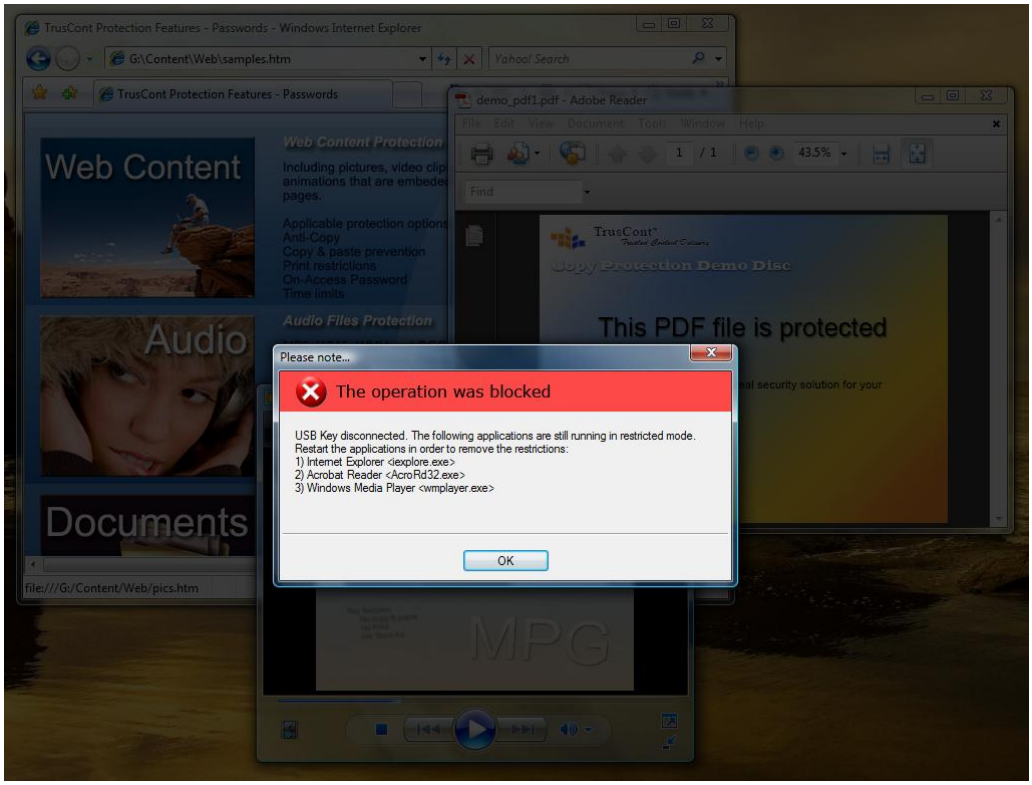
TrusCont Protection Features - Passwords - Windows Internet Explorer
TrusCont Protection Features - Passwords
Web Content
Audio
Documents
demo_pdf1.pdf - Adobe Reader
This PDF file is protected
Please note...
The operation was blocked
USB Key disconnected. The following applications are still running in restricted mode.
Restart the applications in order to remove the restrictions:
1) Internet Explorer <iexplore.exe>
2) Acrobat Reader <AcroRd32.exe>
3) Windows Media Player <wmplayer.exe>
OK
MPG

Figure 13: TSFD Disconnect Notification

Opening Protected Files in Standard 3rd Party Applications

By default, only certified 3rd party applications can be used to open protected files. In case an end user tried to open a protected file with an unsupported application a notification will be displayed indicating which applications are suitable for viewing / playing the specific file type he tries to open (see *Figure 14 below*). In addition, the Toolkit also allows the protected files to be opened in 3rd party applications that are stored on the TSFD itself even if these applications are not included in the certified applications list. However, there is no guaranty that these applications will be able to read the files properly. If you do not wish to allow read access to uncertified applications included in your project you can disable this option in the advanced project options – simply remove the "Generic" application from the list. The "Generic" record represents all uncertified applications included in your project.

It is also possible to configure the Toolkit in order to support other uncertified 3rd party applications that are not included on the TSFD via the advanced options of the 'Project Edit' page. Please refer to *Appendix A – Customizing 3rd Party Applications Support for Content Protection*, for detailed instructions.

For a list of certified applications that are supported by default, please refer to section *5.2.4.5,*

Viewing the List of 3rd Party Applications.

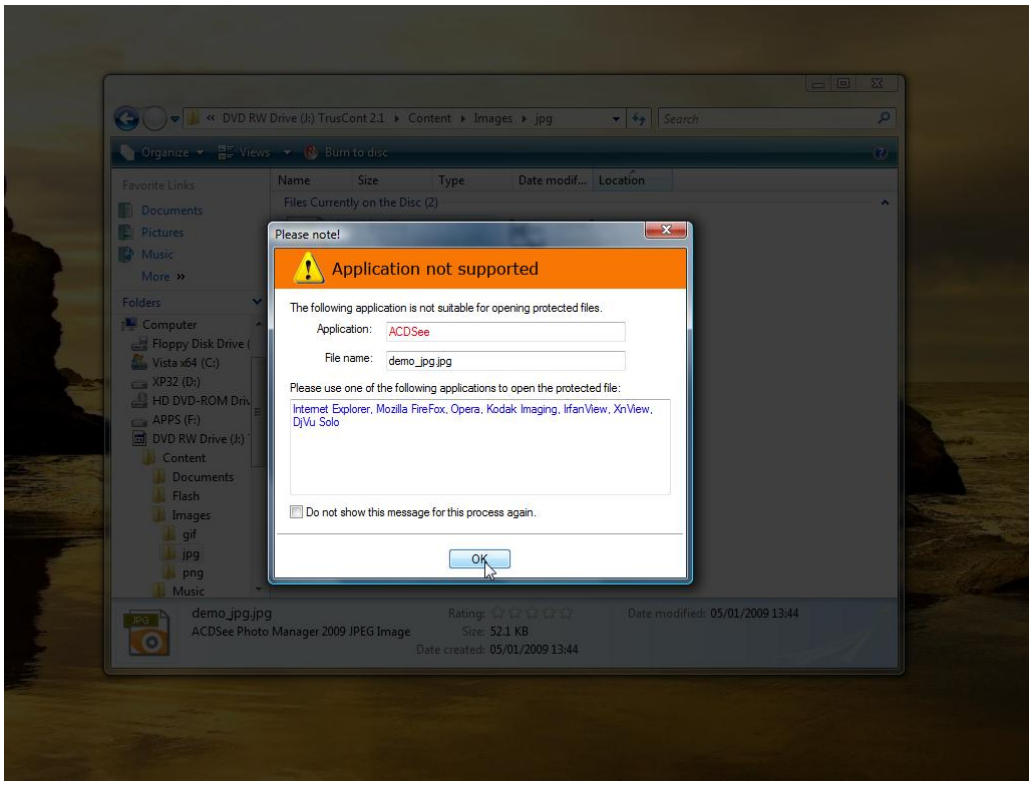
Please note!
Application not supported
The following application is not suitable for opening protected files.
Application: ACDSee
File name: demo_jpg.jpg
Please use one of the following applications to open the protected file:
Internet Explorer, Mozilla FireFox, Opera, Kodak Imaging, IrfanView, XnView, DjVu Solo
Do not show this message for this process again.
OK

Figure 14: Opening Protected Files with Unsupported Applications

2.2.1 Operating Systems Compatibility for Running Protected Content Files

TrusCont copy protection for content files is compatible with the following operating systems:

Windows 2000 SP4 with Rollup 1

Windows XP SP2, SP3

Windows XP x64 SP1, SP2

Windows Vista SP1

Windows Vista x64 SP1

Windows Server 2003

Windows Server 2003 x64

Windows Server 2008

Windows Server 2008 x64

Windows 7

Windows 7 x64

2.3 Protection of Software, and Content Files on the Same Disk

A TSFD may contain both protected program files, and protected content files. TSFDs containing only protected program files will look identical to their unprotected source (in terms of number of files and file names). TSFDs containing protected content files include an additional Autorun file named 'RunMe.exe' as described in section *2.2 above*.

TSFDs containing both protected program files and protected content files will also include the TrusCont Autorun file (RunMe.exe by default). This file is designed to run automatically upon connecting the TSFD to the host computer. If the Autorun feature on the host computer is disabled, then this file needs to be run manually in order for the protected content files to function properly. However, protected program files stored on the same TSFD do not require the TrusCont Autorun file and can run normally even if it doesn't run first.

Important note: Program files recorded on the same TSFD that are used to read protected content files must be left unprotected. Otherwise the program files protection and content protection may conflict.

2.4 Local Administrator Rights

Running protected files requires local administrator rights. It is currently not possible to run files protected on TSFDs under restricted accounts.

Important note: by default all home users have local administrator rights. In some corporate environments users may have restricted accounts. TSFDs require the end users to have only local administrator rights, administrator rights for the network is not required.

3. Choosing Protection Strategy

Give some thought to your copy protection strategy before recording your content to TSFD devices:

- Identify the most valuable files that require protection – in software this may be the main executable file. In e-learning materials, service manuals, etc. this may be documents or flash animations.
- Protect only the valuable files that require protection – Generic files such as 3rd party applications, files without commercial value or files without sensitive content shall be left unprotected. Protecting files (especially content files) without reason just limits their functionality and operating environment for no reason.
- Decide which operations you wish to restrict – a strict security policy provides good protection for your content. However, some publishers choose to enable operations such as printing to allow their customers easier and more convenient use.
- Add password protection to restrict access of the protected content to specific subscribers.
- Set different passwords to different data sets stored on the same TSFD to target different data sets to different subscribers/divisions.
- Set expiration dates if your content is valid to a specific period, or if using outdated content you publish is not desired.

You are now ready to install the TSFD Protection Toolkit and protect your content.

4. Installing TrusCont TSFD Protection Toolkit

4.1 System Requirements

Before starting the installation process, please make sure your system meets the following minimum system requirements:

- Pentium III or higher CPU
- 30Mb of free Hard Disk space
- 10Gb of free Hard Disk space for temporary files during the production process
- 512 MB of system memory (RAM). 2GB recommended.
- USB 2.0 interface
- Internet Explorer 6.0 or higher
- Adobe Acrobat / Acrobat reader required to view this user manual
- **Supported OS:** Windows XP Service Pack 2, Windows XP x64, Windows Vista, Windows Vista x64, Windows 7, Windows 7 64-bit, Windows Server 2003, Windows Server 2003 64-bit, Windows Server 2008, Windows Server 2008 64-bit

4.2 Starting the installation

TrusCont TSFD Protection Toolkit installation package consists of a single installation file. To obtain a copy of the Toolkit installation file, contact your local TrusCont representative or refer to TrusCont website (http://www.truscont.com). To start the installation process, save the installation file to your local Hard Disk and double click it. Follow the on-screen instruction to complete the installation. The installation process will automatically create shortcuts to the Toolkit on your desktop and in the programs menu. Click one of the shortcuts to start the program. Please note that running multiple instances of the software at the same time is not supported.

5. Using TrusCont TSFD Protection Toolkit

5.1 Overview

The TSFD Protection Toolkit allows you to protect and publish your valuable content on TSFD devices using just a few simple steps:

- **Creating a Project** – The first step is creating a "project", which defines your publication to the Toolkit – the files you wish to publish, which files to protect, etc.
- **Saving a Project for Future Use** – After creating a project you can save it for future productions. This allows you to start or resume production of the same project at a later stage without repeating the creation process.
- **Starting Duplication** – Start recording your new project (or a saved project) to TSFD devices.
- **Creating & Recording an Image** – Creating an image is another method for saving a project for future production. Recording from an image provides better performance than recording from a saved project but once created it cannot be changed.

5.2 Creating a New Project

5.2.1 Preparing Your Content

To ensure proper creation of your project, please organize your content using the following guidelines:

- ☒ Verify the functionality of your title – The TSFD protection process doesn't change the functionality of your files in any way. Verify that your title works as planned before using the Toolkit.
- ☒ Organize your files on your local computer – Using files stored on removable drives is blocked in order to avoid potential interruptions of the project creation process due to potential connectivity failures.
- ☒ Make sure your files are not being used – Make sure your project files are not open in any other software and remain unchanged through the project creation process.
- ☒ Do not use files that are already protected – Files recorded on TSFD devices may already be protected. It is not possible to reapply the copy protection on files that are already protected. Always use source files located on your computer.

5.2.2 Starting a New Project

Open TrusCont TSFD Protection Toolkit and follow these simple instructions:

A. Wait for the welcome page to appear then click next.

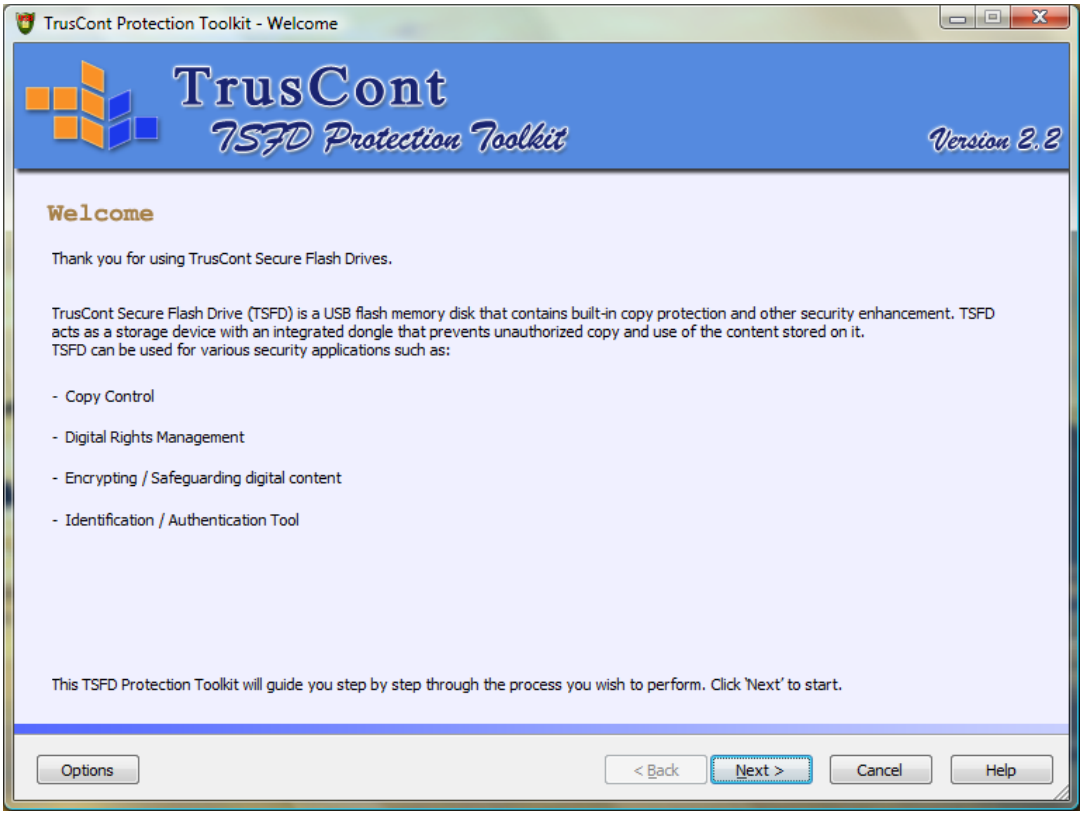
TrusCont Protection Toolkit - Welcome
TrusCont
TSFD Protection Toolkit
Version 2.2
Welcome
Thank you for using TrusCont Secure Flash Drives.
TrusCont Secure Flash Drive (TSFD) is a USB flash memory disk that contains built-in copy protection and other security enhancement. TSFD acts as a storage device with an integrated dongle that prevents unauthorized copy and use of the content stored on it.
TSFD can be used for various security applications such as:
- Copy Control
- Digital Rights Management
- Encrypting / Safeguarding digital content
- Identification / Authentication Tool
This TSFD Protection Toolkit will guide you step by step through the process you wish to perform. Click 'Next' to start.
Options
< Back
Next >
Cancel
Help

Figure 15: The Welcome Page

B. On the 'Select Task' page select 'New Project' then click next.

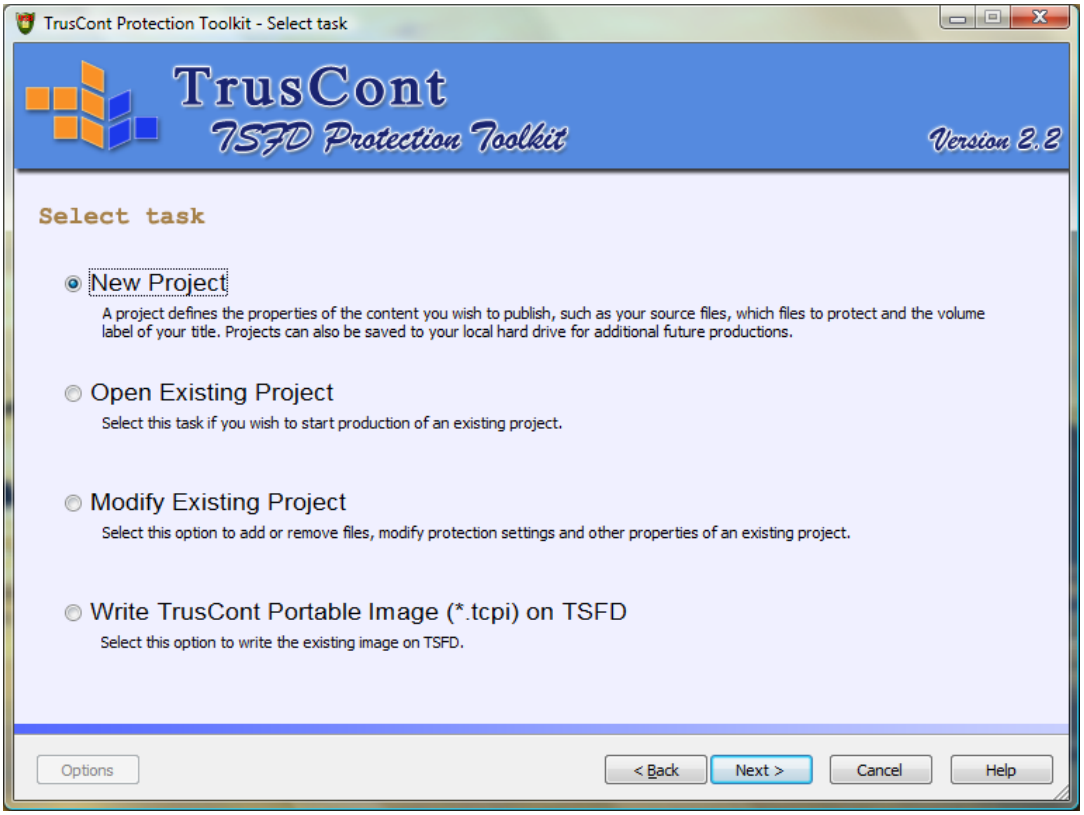
TrusCont Protection Toolkit - Select task
TrusCont
TSFD Protection Toolkit
Version 2.2
Select task
New Project
A project defines the properties of the content you wish to publish, such as your source files, which files to protect and the volume label of your title. Projects can also be saved to your local hard drive for additional future productions.
Open Existing Project
Select this task if you wish to start production of an existing project.
Modify Existing Project
Select this option to add or remove files, modify protection settings and other properties of an existing project.
Write TrusCont Portable Image (*.tcpi) on TSFD
Select this option to write the existing image on TSFD.
Options
< Back
Next >
Cancel
Help

Figure 16: Select Task Page

C. The 'Edit Project' page will appear. Proceed to the next section, *Editing a Project,* to add files and folders to your project.

5.2.3 Editing a Project

The 'Edit Project' page has two main panels. The left panel is a tree view of all the files and folders on your project. These are the files and folders that will eventually be recorded to the TSFD devices. The right panel contains a table that lists only the files of your project corresponding to the supported file types. These are the files on your project that can be protected.

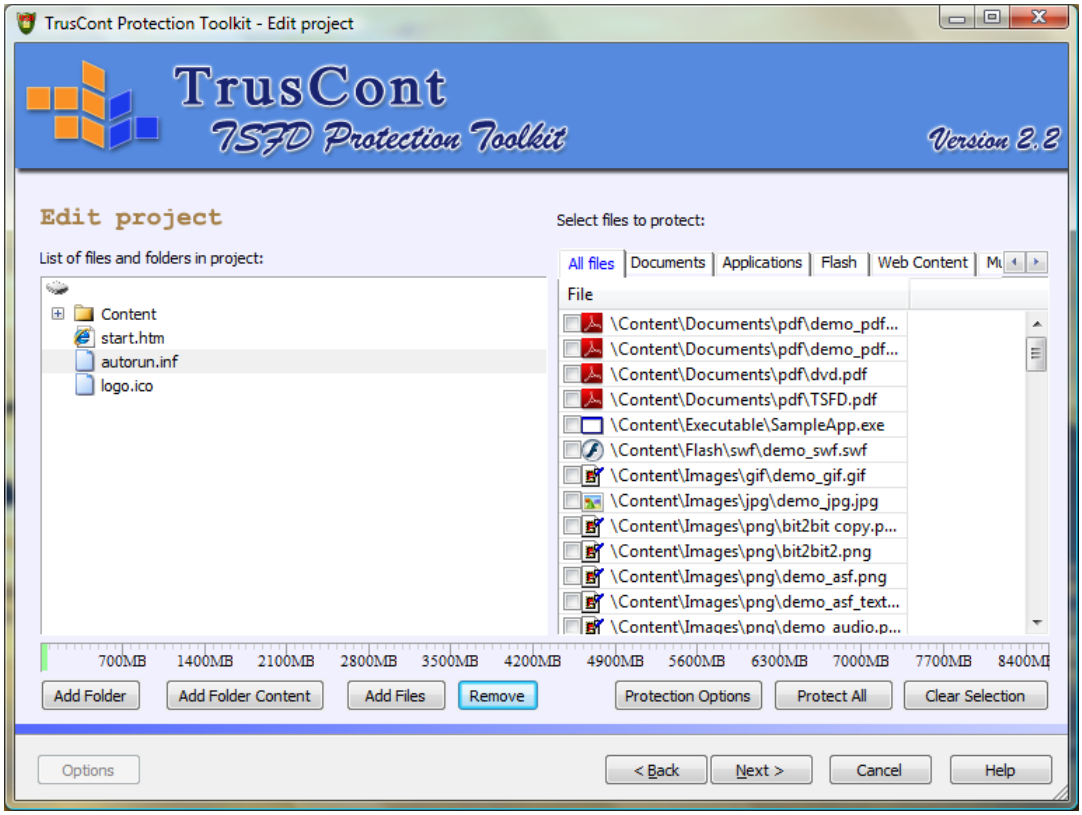

Figure 17: The Edit Project Page

The right panel is diveded into tabs based on the different file types that you add to your project. For example, clicking on the 'Web Content' tab populates the table only with web file types such as HTM and HTML files. By default, the 'All files' tab is selected. This tab displays all the files of all types on your project that can be protected.

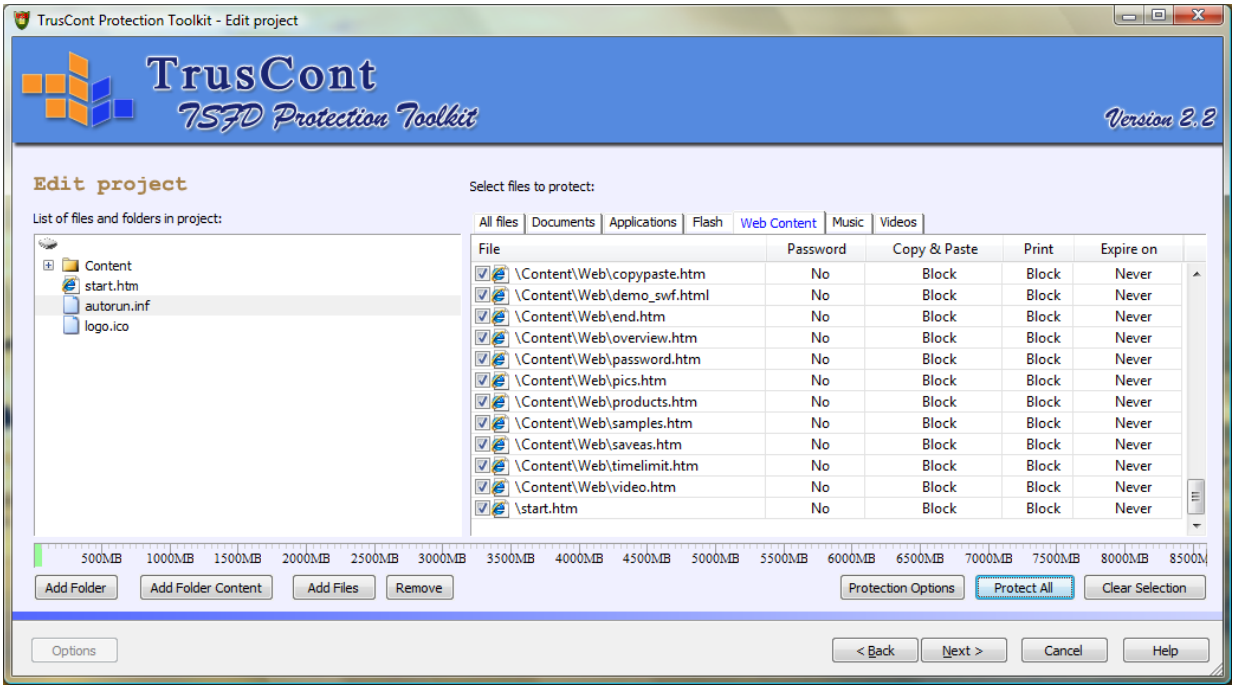

Figure 18: Tabs in the Edit Project Page

The columns of the table specify the copy protection options for each individual file that is marked for protection. These columns appear only when selecting files to protect.

Use the instructions in the following subsections to edit your project then click next to proceed.

5.2.3.1 Adding Files and Folders

There are three methods for adding files and folders to your project – Adding a folder, adding a folder contents and adding files. Each can be achieved by clicking the corresponding button at the bottom of the page (see *Figure 18 above*).

Add Folder – Use this button to add an entire folder, including all its files and sub-folders to your project. The 'Add Folder' dialog box will appear. The folder will be added under the folder that is selected on the left panel. If you wish to add the folder to the root of your project, select the disk icon. Otherwise select the sub-folder under which you wish to add another folder.

Add Folder Contents – Use this button to add an entire folder contents. The contents of the folder that you select will be added under the folder that is selected on the left panel, but the folder itself will not be created.

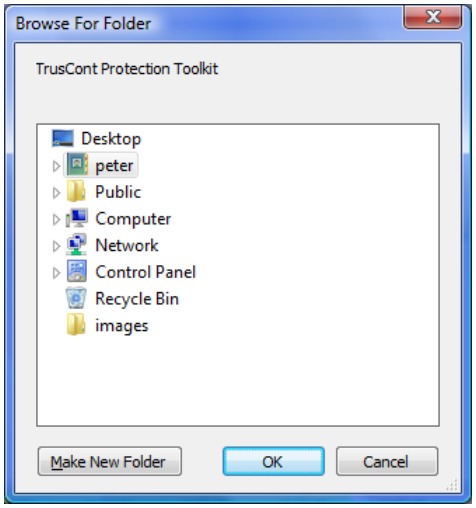

Figure 19: Add Folder Dialog

Add Files – Use this button to add files to a folder within your project. The 'Add Files' dialog will appear. Select the files you wish to add and click 'Open'. The files you select will be added under the folder which is selected on the left panel.

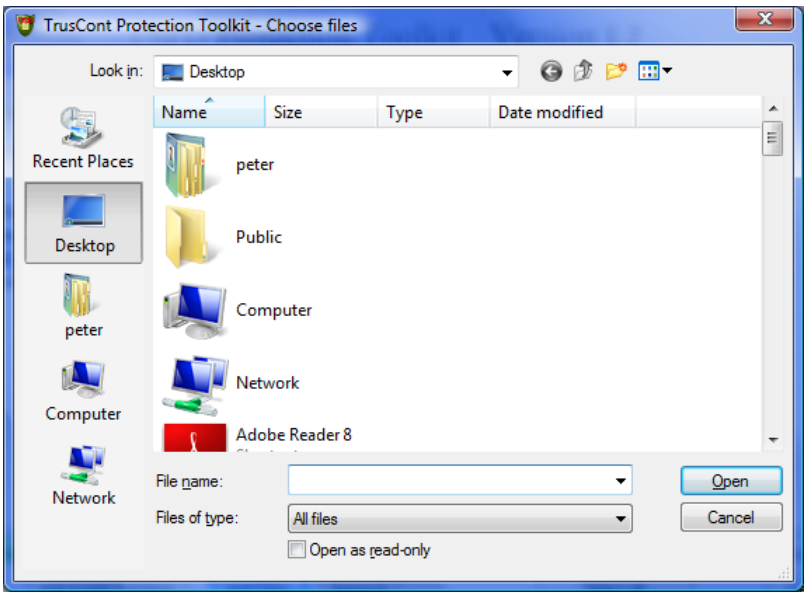

Figure 20: Add Files Dialog

5.2.3.2 Removing Files and Folders

To remove files or folders from your project, select the file or folder you wish to remove and then click the 'Remove' button. You can also right-click any file or folder on the left or right panels and click 'Remove' from the popup menu.

5.2.3.3 Marking Files for Protection

While the left panel of the 'Edit Project' page lists all the files and folders of your project, the right panel lists only the files that can be protected using the Toolkit. When the root folder on the left panel (the disk icon) is selected, the right panel lists all the protectable files of your project. When a sub-folder is selected, the right panel lists only the protectable files within the selected folder and the sub-folders under it.

On the right panel, check the boxes next to the files that you wish to protect. These files will be functional only if the TSFD device on which they are recorded is connected to the end user's computer. The rest of the files will remain unprotected and the end user will be able to copy and use them from his local Hard Drive even if the TSFD device is not connected to his local computer.

To select all files listed on the right panel, click the 'Protect All' button. The 'Protect All' button marks all the files within the selected tab. To clear all selections within the specific tab click the 'Clear Selection' button.

5.2.3.4 Protecting Digitally Signed Program Files

Some files may be digitally signed. Digital signatures are often used on program files for various purposes such as validating the file's content. When applying copy protection to program files, the files are changed. If the files are digitally signed, then digital signature can no longer be used in order to validate the file. The functionality of the file is not affected. However, some operating systems, such as Windows Vista and Windows XP may require end users for confirmation of running the protected files.

5.2.3.5 Customizing Copy Protection Options for Individual Program Files

It is also possible to customize the copy protection behavior for individual files. To customize the copy protection behavior of a specific program file double click the specific file from the right panel, or right-click the file and select 'Option' from the pop-up menu.

Protection box title

Whenever a user tries to run a protected file without the original TSFD connected, the protection system displays a message box containing a standard error message. This field allows you to customize the title text of this message box.

Protection box text

This field allows you to change the text of the message that will be displayed whenever a user tries to run the protected file without the original TSFD connected to his computer.

Allow execution from another media

This option is enabled by default. It allows the end user to copy the protected files to his local Hard Drive or any other media for performance or other purposes. However, the original TSFD must be connected to the local computer in order to run the file. If this option is turned off, the user can run the protected file only directly from the original TSFD.

Background Checks

This option is disabled by default. If enabled, the copy protection system will perform periodic security checks as long as the protected program file is running. In case the original TSFD is disconnected from the computer, the copy protection system will suspend the operation of the protected program file and display a warning message asking the user to re-plug the original TSFD.

Terminate on Eject

This option is disabled by default. It works in a similar way to the background checks. However, this option causes the protected program to terminate immediately in case the TSFD is disconnected from the computer.

Password

You can also protect your files by using a password. Just type in the password you wish to apply to your file. Whenever an end user will try to run the protected file, the copy protection system will display a dialog box asking for the password.

Important Note: The password cannot start or end with space characters. Spaces at the beginning or/and end of the password are automatically truncated.

Expiration date

Check this option to apply a time limit on your files. Select the date in which your files will expire. After the specified date your files will no longer be usable. Trying to run the protected file after the specified date will display a message indicating the application has expired.

Important note: By default the expiration date is tested against the end user's system clock and also an external time server if an internet connection is available. It is also possible to force the copy protection to use only an external time server. This results in a much stronger time limit but requires the end user to have an internet connection in order to open the protected file. Please refer to section *5.2.4.2, Forcing Time Limit Verification Using External Time Source Only,* for further instructions on enabling this option.

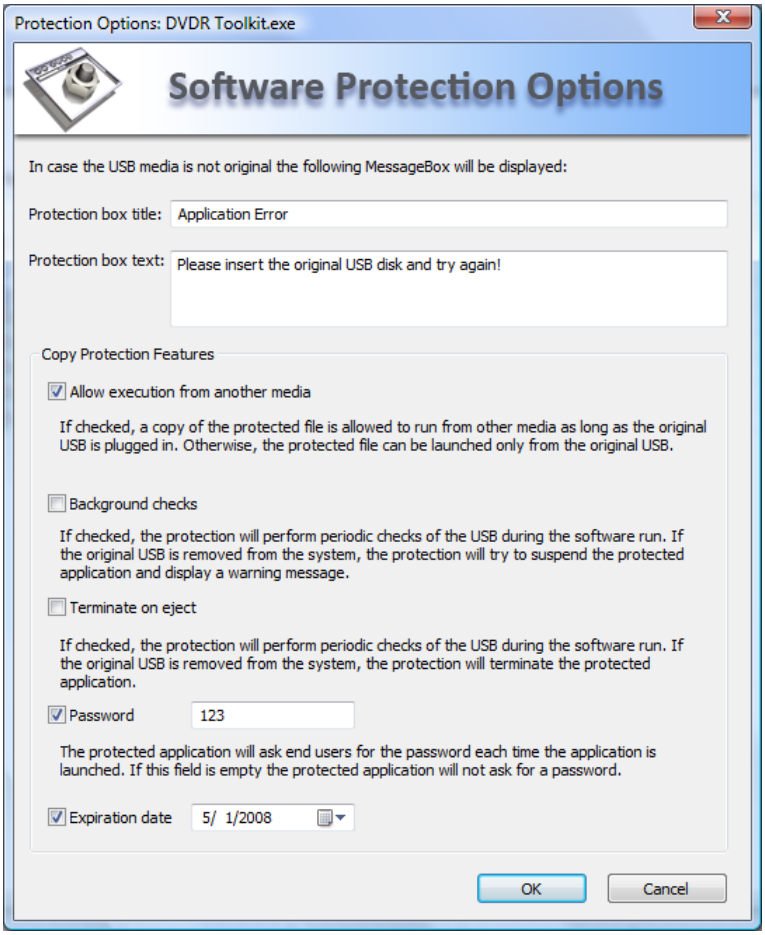
Protection Options: DVDR Toolkit.exe
Software Protection Options
In case the USB media is not original the following MessageBox will be displayed:
Protection box title:
Application Error
Protection box text:
Please insert the original USB disk and try again!
Copy Protection Features
Allow execution from another media
If checked, a copy of the protected file is allowed to run from other media as long as the original USB is plugged in. Otherwise, the protected file can be launched only from the original USB.
Background checks
If checked, the protection will perform periodic checks of the USB during the software run. If the original USB is removed from the system, the protection will try to suspend the protected application and display a warning message.
Terminate on eject
If checked, the protection will perform periodic checks of the USB during the software run. If the original USB is removed from the system, the protection will terminate the protected application.
Password
123
The protected application will ask end users for the password each time the application is launched. If this field is empty the protected application will not ask for a password.
Expiration date
5/ 1/2008
OK
Cancel

Figure 21: Copy Protection Options for Individual Program Files

5.2.3.6 Customizing Copy Protection Options for Individual Content Files

The available copy protection options for each file depend on its type. For example, for music files it is only possible to set a password and expiration date, while for documents it is also possible to set 'Copy & Paste' and 'Printing' restrictions.

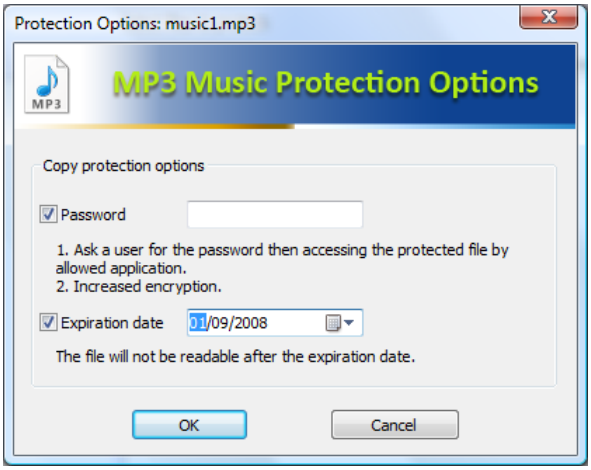
Protection Options: music1.mp3
MP3 Music Protection Options
Copy protection options
Password
1. Ask a user for the password then accessing the protected file by allowed application.
2. Increased encryption.
Expiration date
31/09/2008
The file will not be readable after the expiration date.
OK
Cancel

Figure 22: Copy Protection Options for MP3 Music Files

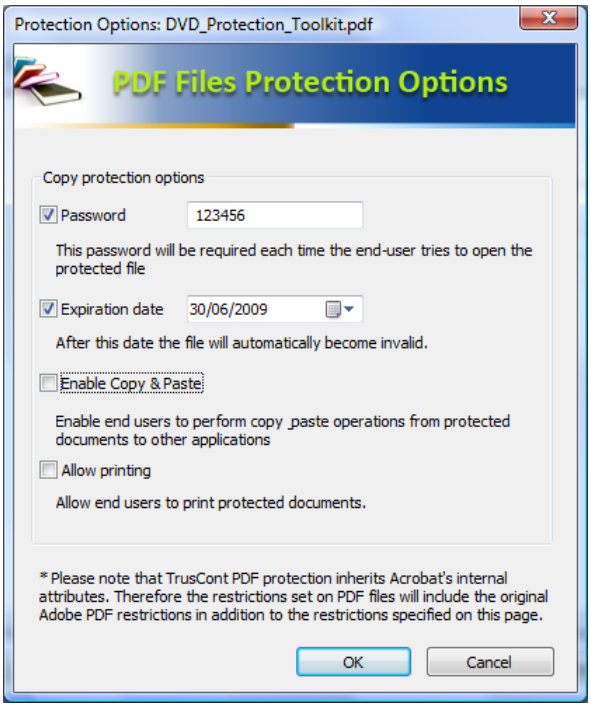
Protection Options: DVD_Protection_Toolkit.pdf
PDF Files Protection Options
Copy protection options
Password
123456
This password will be required each time the end-user tries to open the protected file
Expiration date
30/06/2009
After this date the file will automatically become invalid.
Enable Copy & Paste
Enable end users to perform copy _paste operations from protected documents to other applications
Allow printing
Allow end users to print protected documents.
* Please note that TrusCont PDF protection inherits Acrobat's internal attributes. Therefore the restrictions set on PDF files will include the original Adobe PDF restrictions in addition to the restrictions specified on this page.
OK
Cancel

Figure 23: Copy Protection Options for PDF Documents

Important notes on PDF protection options:

- The Toolkit preserves the original PDF file's security attributes. For example, if the original unprotected PDF file has the printing attribute disabled, then the protected PDF file will also have printing disabled, even if you specifically allow printing in the protection options.

Enable Copy & Paste

This option is disabled by default. If enabled, it allows end users to copy and paste text and images from the protected documents to other applications.

Allow Printing

This option is disabled by default. If enabled it allows end users to print the protected documents.

Password and Expiration Date

Identical to the password and expiration date of program files. See section *5.2.3.5 above*.

5.2.3.7 Copy Protection Options by File Type

The table on the following page lists the available copy protection options for each supported file type.

File Type	Password	Expiration Date	Copy & Paste	Print	Background Checks	Terminate on Eject	Allow Execution from Another Medium
EXE	Yes	Yes	No	No	Yes	Yes	Yes
PDF	Yes	Yes	Yes	Yes	No	No	No
DJVU	Yes	Yes	Yes	Yes	No	No	No
HTM	Yes	Yes	Yes	Yes	No	No	No
HTML	Yes	Yes	Yes	Yes	No	No	No
JPG	Yes	Yes	Yes	Yes	No	No	No
PNG	Yes	Yes	Yes	Yes	No	No	No
GIF	Yes	Yes	Yes	Yes	No	No	No
DCA	Yes	Yes	Yes	Yes	No	No	No
DIC	Yes	Yes	Yes	Yes	No	No	No
IMA	Yes	Yes	Yes	Yes	No	No	No
NEMA	Yes	Yes	Yes	Yes	No	No	No
AVI	Yes	Yes	No	No	No	No	No
ASF	Yes	Yes	No	No	No	No	No
MPG	Yes	Yes	No	No	No	No	No
WMV	Yes	Yes	No	No	No	No	No
FLV	Yes	Yes	No	No	No	No	No
MP3	Yes	Yes	No	No	No	No	No
WMA	Yes	Yes	No	No	No	No	No
MID	Yes	Yes	No	No	No	No	No
WAV	Yes	Yes	No	No	No	No	No
OGG	Yes	Yes	No	No	No	No	No
SWF	Yes	Yes	Yes	Yes	No	No	No

5.2.3.8 Customizing Copy Protection Options for Multiple Files

To set protection options for multiple files, mark the files you wish to protect and click the protection options button. Then, select the file type for which you wish to set the protection options. The popup menu lists only the file types listed in the selected tab. The Toolkit will apply the protection options to all the files of the type you have selected and are marked for protection.

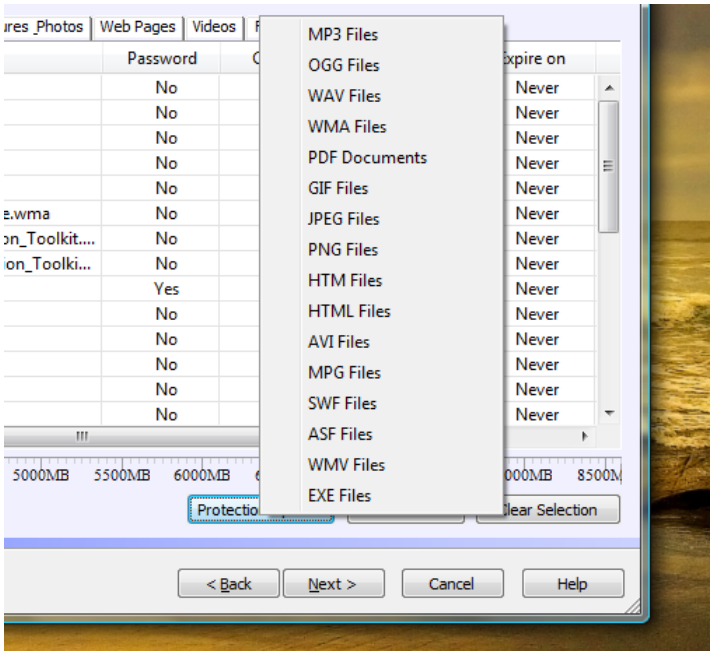

Figure 24: Setting Protection Options for Multiple Files

5.2.3.9 Clearing a Project

To clear your project, right click the disk icon on the left panel and select 'Clear Project' from the popup menu. Selecting this option will remove all the files and folders from your project and clear the list of files to protect on the right panel.

5.2.4 Changing Advanced Project Settings

To access the advanced project settings, right click the disk icon on the left panel and select 'Options'.

Figure 25: Advanced Project Settings

5.2.4.1 Setting a Global Password

Select the options tab, check the 'Set global password for content files' and enter the password you wish to set for your project

Global passwords lock access to all protected content files on your project with one global password that is requested upon connection of the TSFD to the host computer. See section *2.2 above* for additional details on global password behavior.

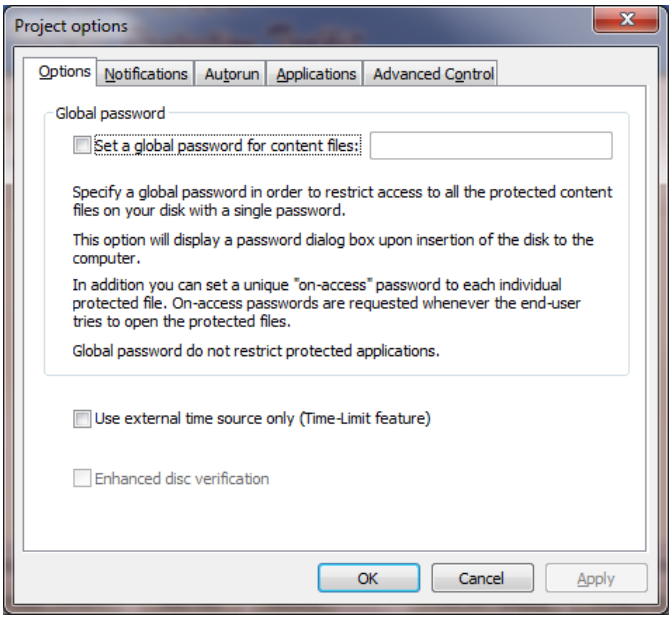
Project options
Options
Notifications
Autorun
Applications
Advanced Control
Global password
Set a global password for content files:
Specify a global password in order to restrict access to all the protected content files on your disk with a single password.
This option will display a password dialog box upon insertion of the disk to the computer.
In addition you can set a unique "on-access" password to each individual protected file. On-access passwords are requested whenever the end-user tries to open the protected files.
Global password do not restrict protected applications.
Use external time source only (Time-Limit feature)
Enhanced disc verification
OK
Cancel
Apply

Figure 26: Setting a Global Password

5.2.4.2 Forcing Time Limit Verification Using External Time Source Only

By default the expiration date is tested against the end user's system clock and also an external time server if an internet connection is available. It is also possible to force the copy protection to use only an external time server. This results in a much stronger time limit but requires the end user to have an internet connection in order to open the protected file. To enable this option check the 'Use external time source only' option.

5.2.4.3 Enabling and Disabling Content Protection Notifications

By default the copy protection system is designed to display notifications to the end users that are triggered by attempts of performing restricted operations (See section *2.2 above* for detailed description of the notifications). The 'Notifications' tab allows the publisher to enable or disabled specific notifications.

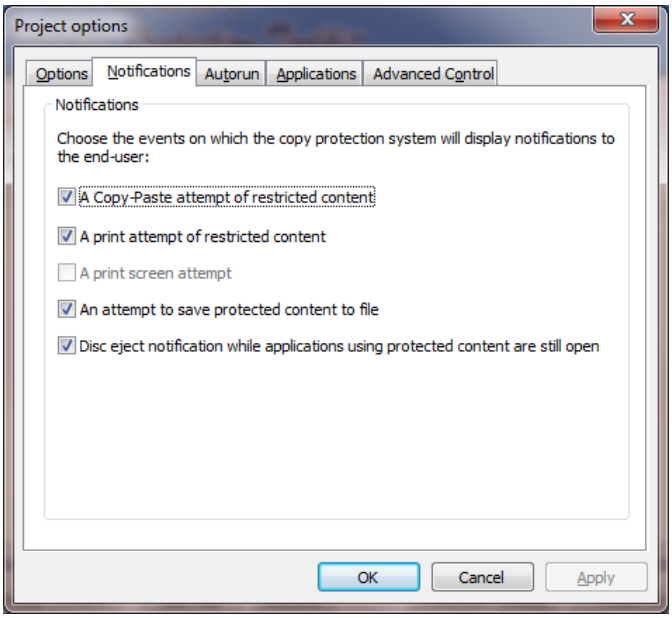

Figure 27: Enabling and Disabling Content Protection Notifications

5.2.4.4 TrusCont Autorun File Name

The default TrusCont Autorun file name that is automatically added to projects with protected content files is "RunMe.exe". The 'Autorun' tab allows the publisher to choose a different file name. The Autorun filename must have only one dot '.' followed by the extension 'exe'. For maximum compatibility, please use only English characters. Autorun name containing non English characters may not start automatically on some systems.

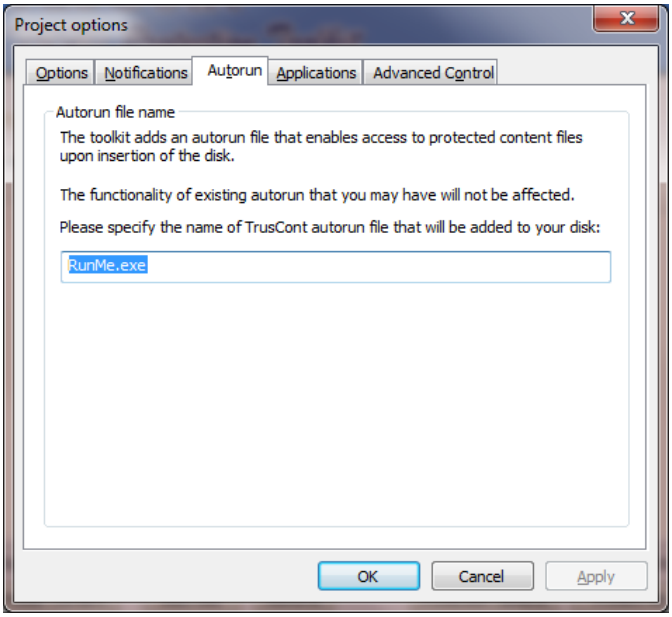
Project options
Options
Notifications
Autorun
Applications
Advanced Control
Autorun file name
The toolkit adds an autorun file that enables access to protected content files upon insertion of the disk.
The functionality of existing autorun that you may have will not be affected.
Please specify the name of TrusCont autorun file that will be added to your disk:
RunMe.exe
OK
Cancel
Apply

Figure 28: Changing TrusCont Autorun File Name

5.2.4.5 Viewing the List of 3rd Party Applications

The 'Applications' tab lists the certified 3rd party applications compatible with TrusCont copy protection system. These are the applications that will be allowed to read the protected files.

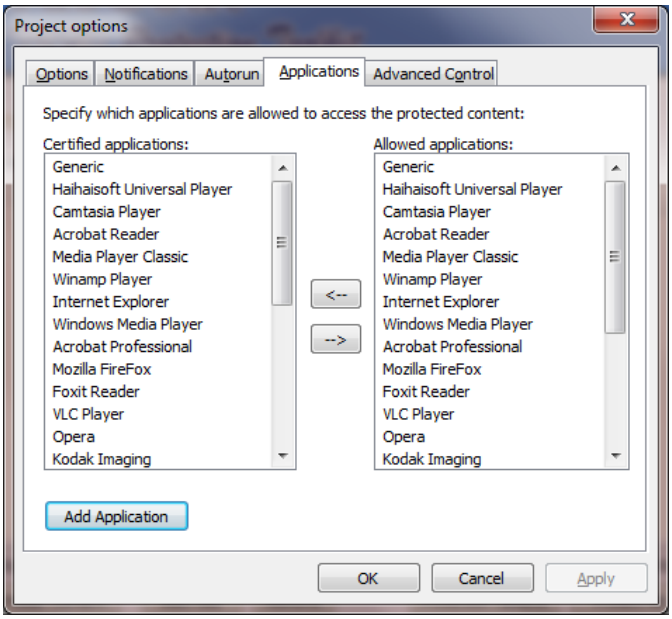

Figure 29: Customizing the List of Allowed Applications

5.2.4.6 Restricting Use of TSFD to Specific Number of Computers, Users, or a Domain

On the 'Advanced Control' tab you can set advanced use restrictions on your product. By default the restriction mode is set to 'None'. This means the resulting disc will be able to run on any computer, user, or a domain even though the content recorded on it cannot be copied.

You can select from the following restriction modes:

a. Computer – set the limit to the number of computers on which each TSFD will be allowed to run. Each TSFD will automatically enable itself on computers on which it is used until the total number of computers exceeds the limit.

b. User – set the limit to the number of users that will be allowed to use each TSFD. In this mode the number of computers on which the TSFD can be used is not restricted. Only the number of users is limited. Each Windows Account is considered a user. For example, on networks with a domain controller a domain user can login with the same account to different computers. Of course,

the TSFD must be connected to the local computer so it is not possible to use the same TSFD on multiple computers at the same time.

c. Domain – This option restricts each TSFD for use only on a single domain. The TSFD is locked to the specific domain on the first use. Then the TSFD can be used only on computers and users of the same domain.

Notes: Setting any one of these restrictions will require end users to have Internet connection for using the protected TSFD for the first time on each computer. Any subsequent runs of the same TSFD on the same computer will not require connection to the internet.

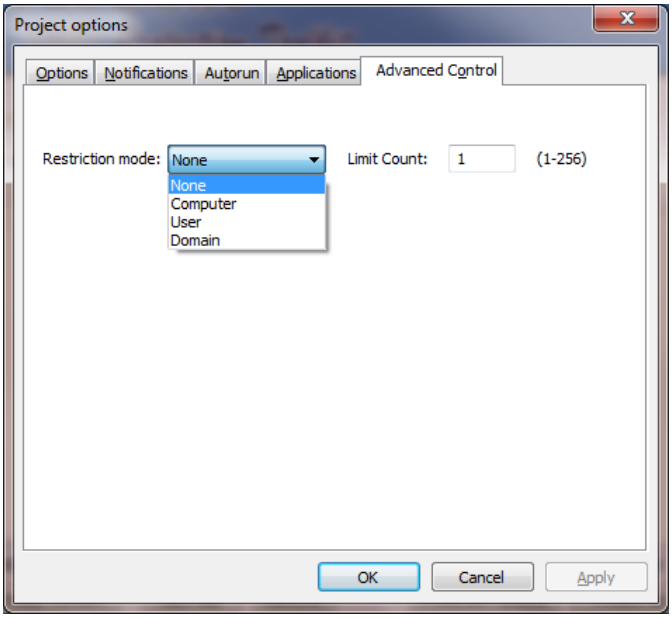

Figure 30: Setting Advanced Use Restrictions

5.2.5 Naming a Project

Once you have finished editing your project, click next to proceed to the 'Volume Information' page.

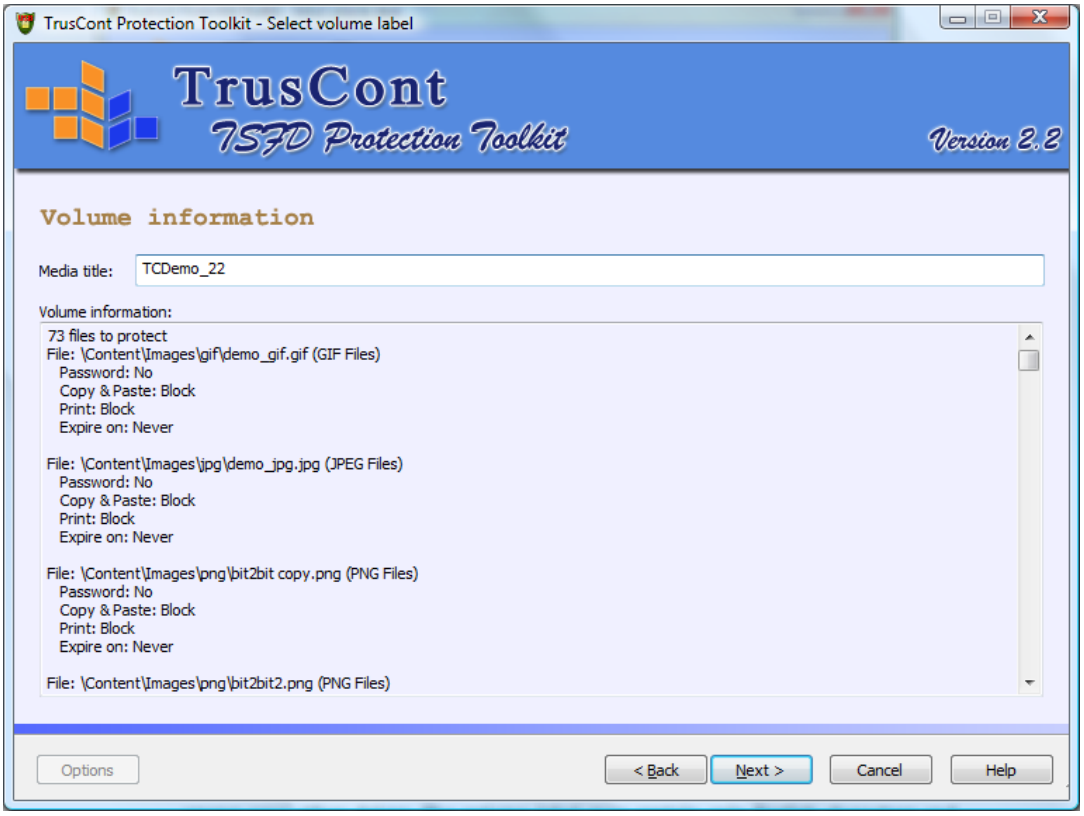

Figure 31: Volume Information Page

The 'Volume Information' page allows you to change the 'Volume Label' (media title). The volume label is the caption that is usually displayed next to the drive letter in windows explorer and 'My Computer'. This helps you or your users to easily locate your TSFD among your other drives. The volume label may contain only English characters and numbers.

5.2.6 Saving & Duplicating Your Project

When you finish creating your project you can start recording it immediately to TSFD devices by selecting the 'Start Duplicating' task (see *Figure 32 below*). For additional instructions on duplicating your project please refer to the instructions in section *5.4 Opening Existing Projects for Duplication*.

You can also save your project for future use in case you plan to record additional TSFD devices with the same content. To save your project, follow the instructions below. Please note that the Toolkit only saves a file that describes your project. Your project's files are not copied from their original location and it is essential that it will not be changed or moved if you wish to use the same project in the future.

1. Select the 'Save Project' option and click next.

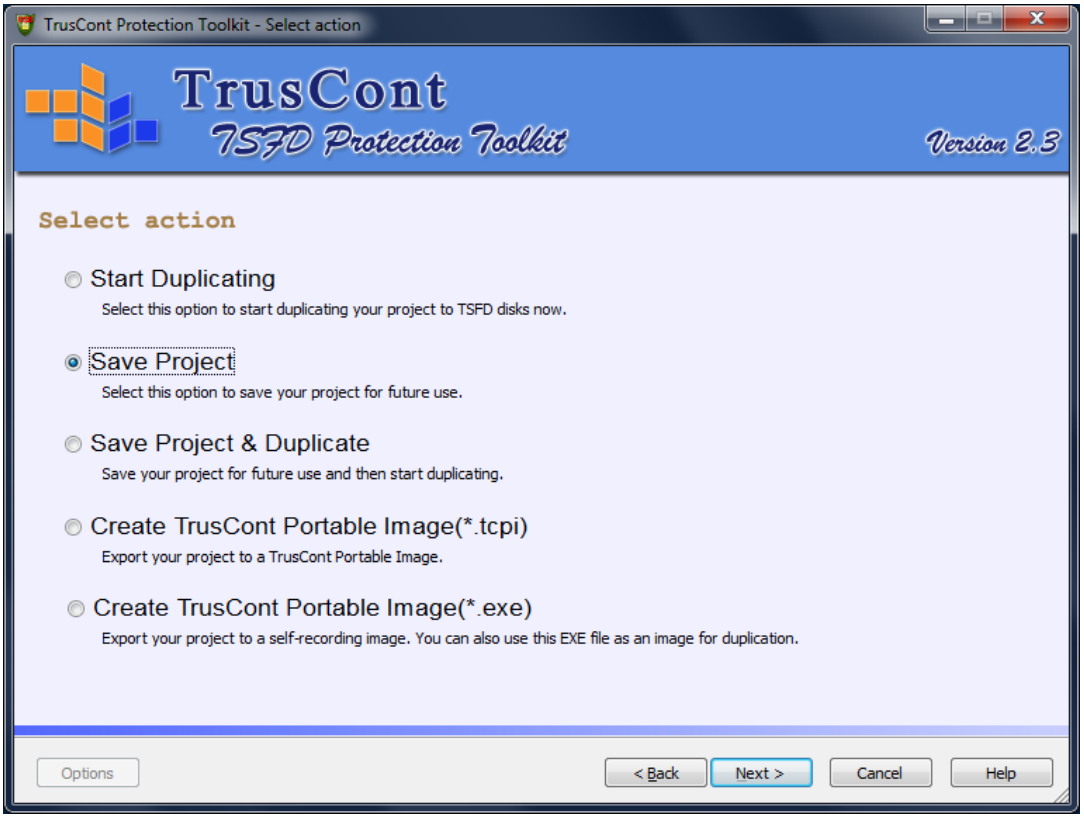
TrusCont Protection Toolkit - Select action
TrusCont
TSFD Protection Toolkit
Version 2.3
Select action
Start Duplicating
Select this option to start duplicating your project to TSFD disks now.
Save Project
Select this option to save your project for future use.
Save Project & Duplicate
Save your project for future use and then start duplicating.
Create TrusCont Portable Image(*.tcpi)
Export your project to a TrusCont Portable Image.
Create TrusCont Portable Image(*.exe)
Export your project to a self-recording image. You can also use this EXE file as an image for duplication.
Options
< Back
Next >
Cancel
Help

Figure 32: Saving and Duplicating New Projects

2. The 'Save Project' page will appear.
3. Click the browse button to open the 'Save As' dialog and select the folder and filename under which your project will be saved.
   Note: Saving to UNC network locations is not supported. Save to local drives only.
4. Click 'Save' on the 'Save as' dialog then click 'Next' on the 'Save Project' page.

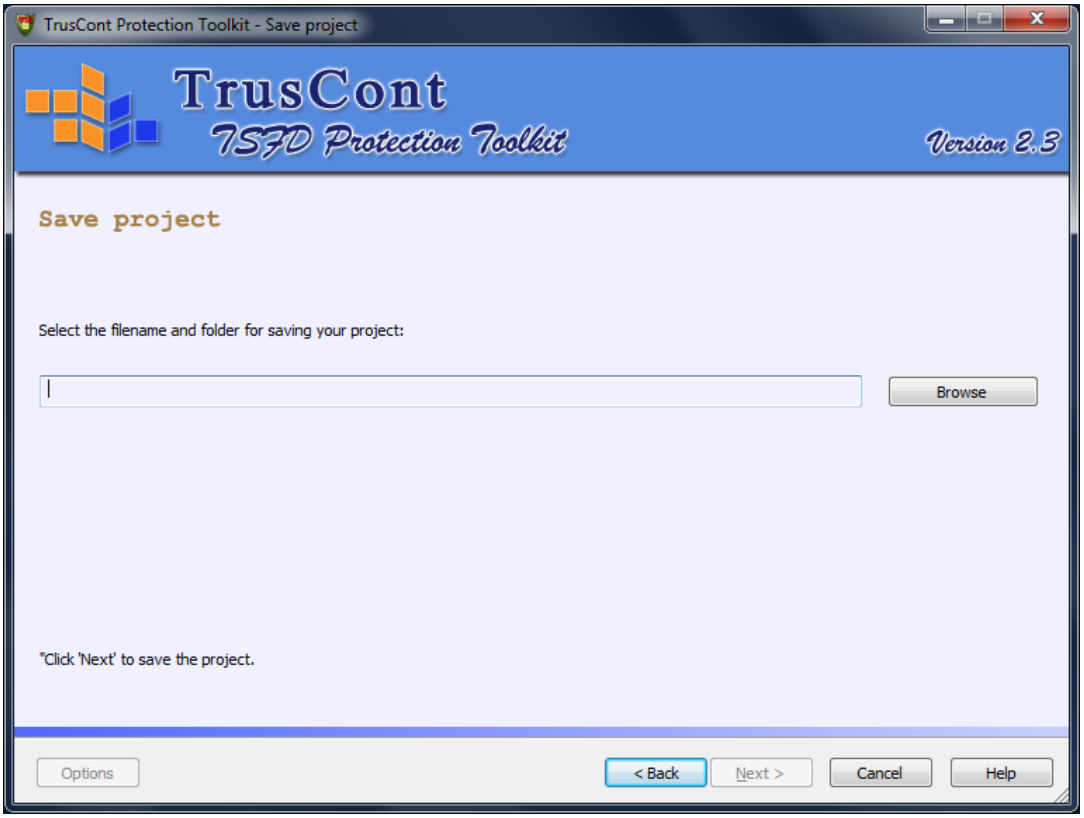

Figure 33: Save Project Page

5.2.7 Creating a Portable Image (*.tcpi)

Exporting your project to a TCPI Portable image is an easy way to save your project for future duplications. Your project is saved in a single data file. Duplicating using an image file provides better performance than duplicating from a project, but once created it cannot be changed. Changes can be performed only by changing the saved project and then creating a new image file.

Duplicating from an image also provides the following benefits:

1. **Interchangeability** – makes your TSFDs interchangeable. This means that a program file from one TSFD can be ran with another TSFD duplicated from the same image. All TSFDs duplicated from the same image are interchangeable. TSFDs duplicated from different images, directly from source files, or from a saved project are not interchangeable.
2. **Updates** – the TSFD Protection Toolkit also allows you to create update files for updating TSFDs that you already sent to customers. One of the update options is to create an update file that updates only TSFDs of a specific product – i.e. TSFDs duplicated from a specific image.

To save your project as a portable image:

1. Select the 'Create TrusCont Portable Image (*.tcpi)' option on the 'Select Action' page and then click next – See *Figure 32 above*.

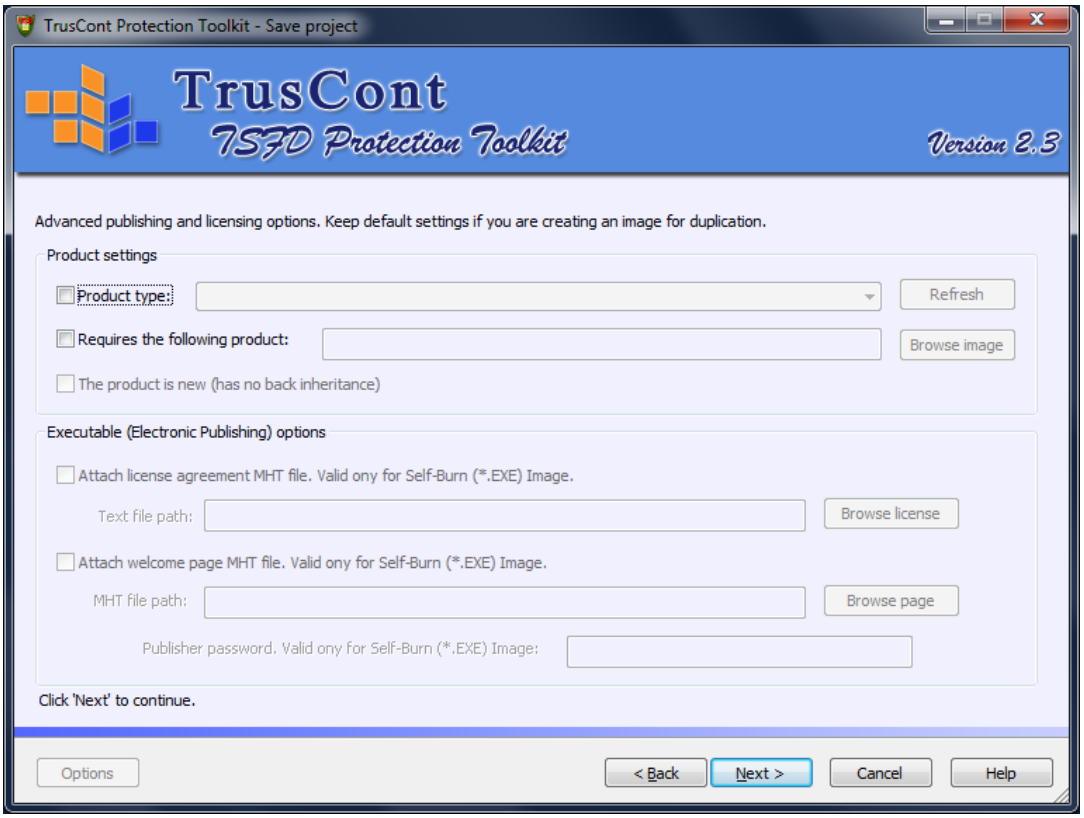
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Refresh
Requires the following product:
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 34: Advanced Publishing & Licensing Options Page

2. The 'Advanced Publishing & Licensing Options' page will open. If you are creating a new image that you intend to duplicate yourself, or at a service provider you trust, keep the default settings and click next to proceed to the 'Save Project' page.

3. Save Project Page Options
   - **File name and location** – click browse to specify file name and folder for saving the portable image.
   - **Image File System CD (UDF) / FAT32** – Select CD (UDF) if you wish to eventually record the image on a read-only CD emulation partition. Select FAT32 to create an image for recording on a standard removable, or read-only partition,
   - **Reserve Space for Protected Partition** – check this option to set the minimum size of the partition on which the image will be recorded. This is useful for preserving space for future updates. For example, if your current data size is 1GB but you plan to publish an update that will increase the total data size to 2GB you should preserve at least 2,000 MB.

- **Force Target USB Partitions** – check this option if you wish to force a specific partition configuration. This partition configuration will be applied to any TSFD on which the image will be recorded.

For additional information on partitions configuration and types please refer to section *5.4.3, Partitions Configuration*.

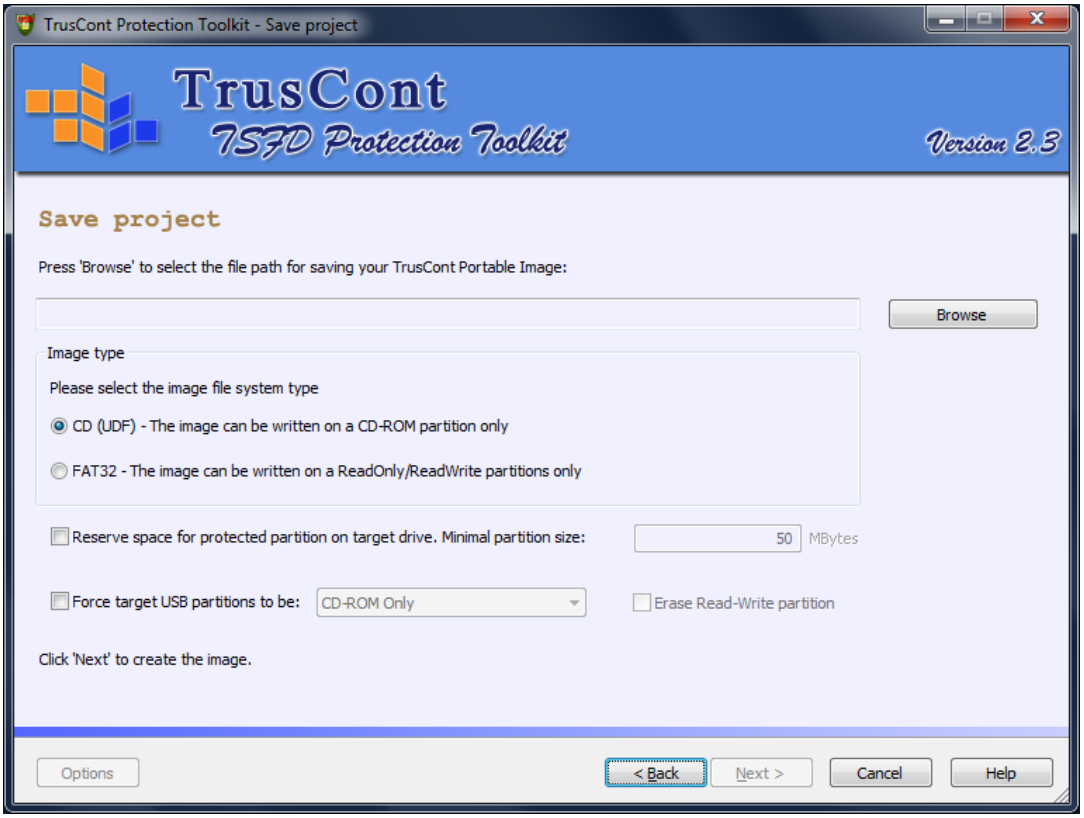
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Save project
Press 'Browse' to select the file path for saving your TrusCont Portable Image:
Browse
Image type
Please select the image file system type
CD (UDF) - The image can be written on a CD-ROM partition only
FAT32 - The image can be written on a ReadOnly/ReadWrite partitions only
Reserve space for protected partition on target drive. Minimal partition size:
50
MBytes
Force target USB partitions to be:
CD-ROM Only
Erase Read-Write partition
Click 'Next' to create the image.
Options
< Back
Next >
Cancel
Help

Figure 35: Creating a Portable Image

5.2.8 Creating a Portable Image (*.exe)

The Toolkit also allows you to create a 'self-recording' image compiled into an EXE file. This is an image that can actually record itself to a TSFD without requiring the Toolkit or any other duplication tools. Self-recording EXE images are useful mainly for sending updates for TSFDs you already sent to customers. Send the EXE file to your customers, or make it available for download. Your customers will be able to run the executable and it will automatically overwrite their TSFD with the updated content.

Please refer to section *8 Updating Content on TrusCont Secure Flash Drives* for instructions on creating update files.

5.3 Modifying Saved Projects

To modify an existing project follow these simple instructions:

A. Run the Toolkit, wait for the welcome page to appear then click 'Next'.

B. Select 'Modify Existing Project' and click 'Next'.

C. Click 'Browse', select the project you wish to modify then click 'Next'.

D. Refer to section *5.2.3 Editing a Project* for additional instructions on editing your project.

Note: A saved project should be used only with the same version of the Toolkit used to create it.

5.4 Opening Existing Projects for Duplication

A. Run the Toolkit, wait for the welcome page to appear then click 'Next'.

B. On the 'Select Task' page choose 'Open Existing Project' and click 'Next'.

C. The 'Open Project' page will appear. Click 'Browse' to select the project you wish to duplicate.

D. Click 'Next' to move to the 'Select Target' page.

Note: A saved project should be used only with the same version of the Toolkit used to create it.

5.4.1 Selecting the Target TSFD device

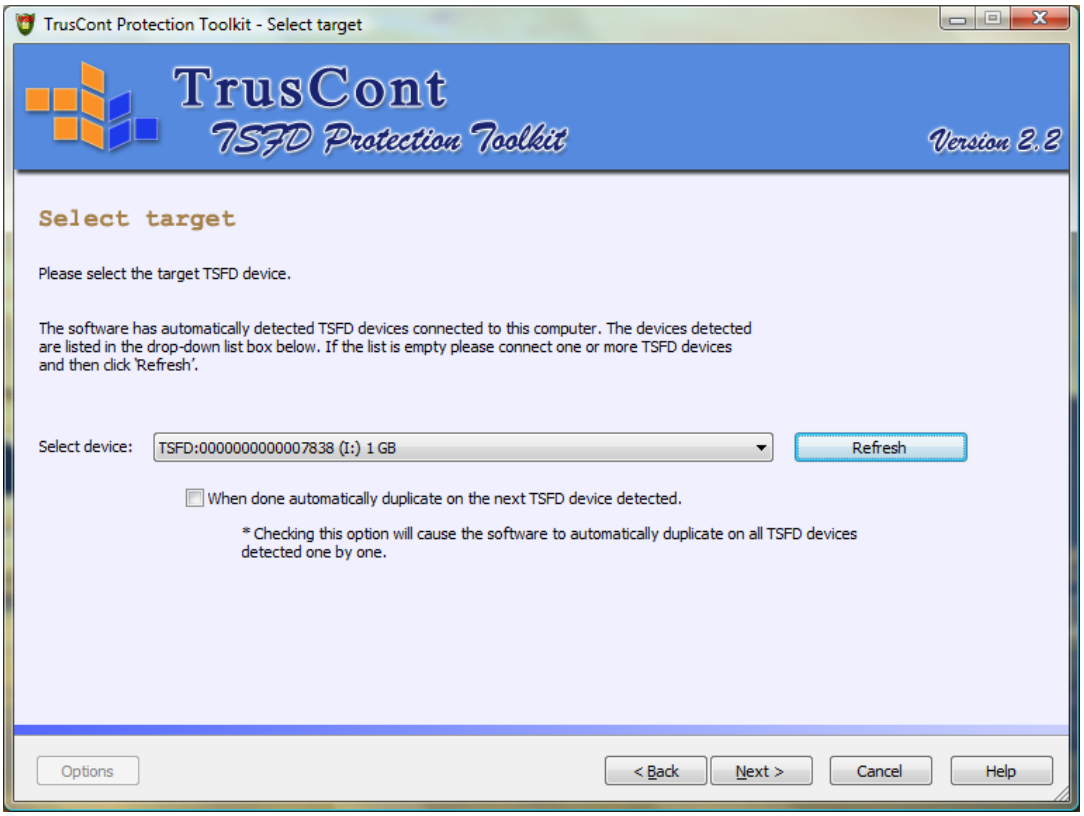
TrusCont Protection Toolkit - Select target
TrusCont
TSFD Protection Toolkit
Version 2.2
Select target
Please select the target TSFD device.
The software has automatically detected TSFD devices connected to this computer. The devices detected are listed in the drop-down list box below. If the list is empty please connect one or more TSFD devices and then click 'Refresh'.
Select device:
TSFD:0000000000007838 (I:) 1 GB
Refresh
When done automatically duplicate on the next TSFD device detected.
* Checking this option will cause the software to automatically duplicate on all TSFD devices detected one by one.
Options
< Back
Next >
Cancel
Help

Figure 36: Select Target Page

The Toolkit automatically detects all TSFD devices connected to your host computer. The devices detected are listed in the drop-down list box next to the 'Select Device' label. If the list is empty, connect one or more TSFD devices to your computer and click 'Refresh'.

Note: TSFD devices are not visible when running the Toolkit under the windows Guest account.

5.4.2 Duplicating on Multiple Devices

If you wish to record more than one device in a single process, check the checkbox with the label 'When done automatically duplicate on the next TSFD device detected'. Please note that the free standard edition of the Toolkit will automatically duplicate on all detected TSFDs, but one at a time. TrusCont also provides a professional edition of the Toolkit that duplicates on multiple devices in parallel. The professional edition is not free and can be purchased via the TrusCont secure online shop.

5.4.3 Partitions Configuration

The TSFD Protection Toolkit enables you to divide the TSFD memory into 2 separate partitions. The first partition is where your project files will be stored. The first partition can be configured as a CD-ROM partition, a read-only partition or a read/write partition. If the first partition is configured as a CD-ROM partition or a read only partition, a second read/write partition can be configured.

TrusCont Protection Toolkit - Select partitions
TrusCont
TSFD Protection Toolkit
Version 2.2
Select target
Please select the type of partition on which you wish to store your files:
1. If the 'Read Only Partition' is checked your files will be stored on a single read only partition.
2. If the 'Read/Write Partition' is checked your files will be stored on a single write enabled partition. Please note that this option allows users to delete your files.
3. If both options are checked your TSFDs will have one read only partition and one write enabled partition. Your files will be stored on the read-only partition and the write enabled partition will be left empty for end users' applications.
You can also specify a CD-ROM partition instead of a Read Only partition. A CD-ROM partition functions similar to a Read Only partition, only it identifies itself to the Windows operating system as a CD-ROM drive. This also enables true Autorun functionality.
Please note that the Toolkit automatically sets the size of read only partitions to the minimum size required in order to hold your files. In this case the size of the write enabled partition is automatically set to the total remaining memory capacity.
Partitions configuration
CD-ROM Partition
Read Only Partition
Read/Write Partition
Publisher password
Set a publisher password to prevent 3rd parties from overwriting your TSFD using the toolkit.Leave this field empty to disable the publisher password feature.
123456
Options
< Back
Next >
Cancel
Help

Figure 37: Partitions Configuration & Publisher Password Page

5.4.3.1 CD-ROM Emulation & Autorun Support

If the first partition is configured as a CD-ROM, the first partition of the TSFD will be detected as a CD-ROM when connecting it to a computer. Your project files will automatically be stored on the CD-ROM partition. Since CD-ROM is a read only medium, your files cannot be deleted.

Windows operating systems have an Autorun feature enabled by default for CD-ROM devices. This enables you to set an Autorun feature on your TSFD by simply including an autorun.inf file in your project.

Important note: When protecting content files it is recommended to set the first partition as a CD-ROM partition. CD-ROM partitions provide a true Autorun functionality ensuring the TrusCont Autorun launches properly.

5.4.3.2 Read Only Partitions

The read only partition option protects your files from deletion. You cannot have both read only and CD-ROM partitions on the same device. If you check the read only partition, the CD-ROM partition will automatically be cleared.

5.4.3.3 Read Write Partitions

If only a single read/write partition is selected the Toolkit will automatically allocate the total capacity of the TSFD to a single read/write partition and store your project files on it. If you choose to configure a read only or a CD-ROM partition in addition to the read/write partition, the Toolkit will first allocate to the read only or CD-ROM partition the minimum capacity required to store your project's files on it. The remaining capacity will then be allocated to the read/write partition.

5.4.3.4 Possible Partitions Configurations

The following table lists all the possible partitions configurations. Please note that your project's files will always be stored on the first partition regardless of its type. The second partition you may configure will not contain any files.

#	Partition 1	Partition 2
1	Read-Only	--
2	Read/Write	--
3	CD-ROM	--
4	Read-Only	Read/Write
5	CD-ROM	Read/Write

5.4.4 Setting a Publisher Password

Each TSFD device includes a 1 year unlimited license for reloading protected content using the TSFD Protection Toolkit. This means that publishers can reuse their TSFD devices as many times as they wish for 1 year. To prevent 3rd parties from reusing your TSFDs you can set a 'Publisher Password' (See *Figure 37 above*). This password can be set only once and is required for future reloading of content to the TSFD device. If a Publisher Password is not yet set on the specific TSFD device, it will be set to the password provided. Otherwise the password provided will be verified against the password set in each TSFD device. In case the password is not correct the recording process fails with an error set to 'incorrect publisher password'.

5.4.5 Confirming Overwrite and Starting the Duplication

Before starting the duplication process the Toolkit displays a standard warning message indicating all TSFD devices on which you record will be overwritten and all information that may be contained in it will be permanently deleted. Click 'Next' to confirm and start the duplication process.

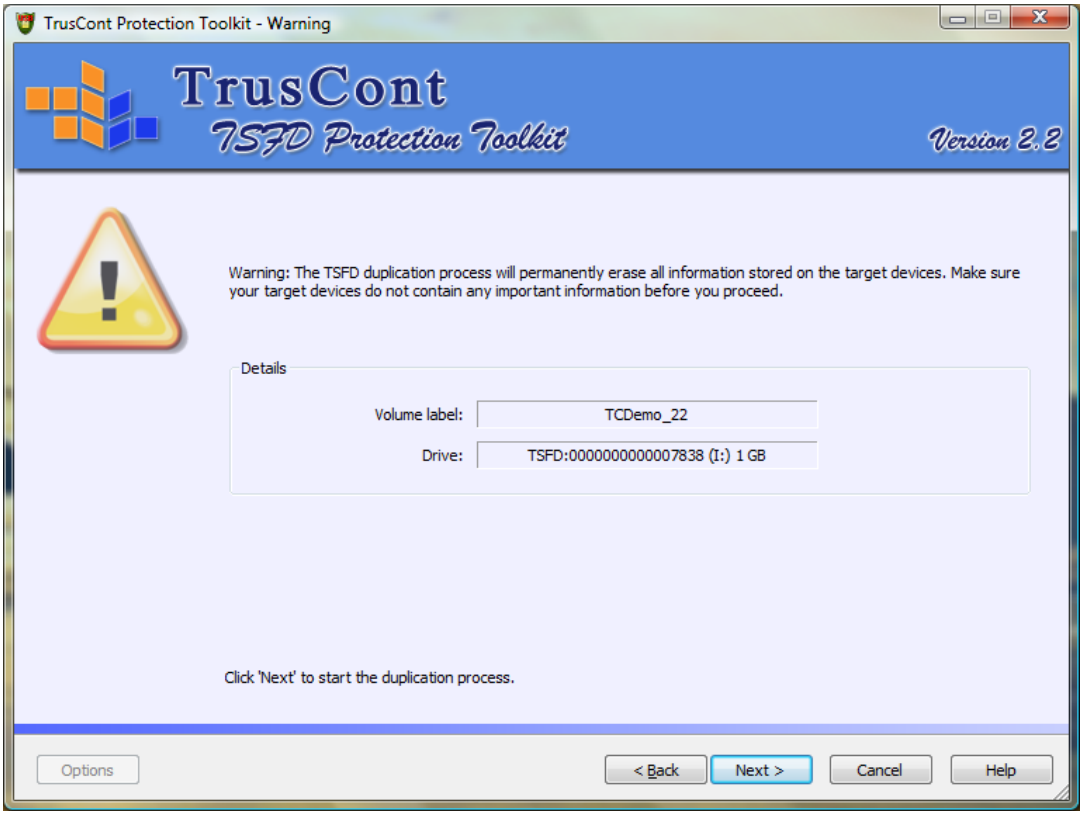
TrusCont Protection Toolkit - Warning
TrusCont
TSFD Protection Toolkit
Version 2.2
Warning: The TSFD duplication process will permanently erase all information stored on the target devices. Make sure your target devices do not contain any important information before you proceed.
Details
Volume label:
TCDemo_22
Drive:
TSFD:0000000000007838 (I:) 1 GB
Click 'Next' to start the duplication process.
Options
< Back
Next >
Cancel
Help

Figure 38: Overwrite Warning Page

Wait for the recording process to finish. If you choose to duplicate on multiple devices, at the end of each recording session the Toolkit will automatically start recording on the next device it detects until no more TSFD devices can be detected. Of course you can interrupt the recording loop at any time.

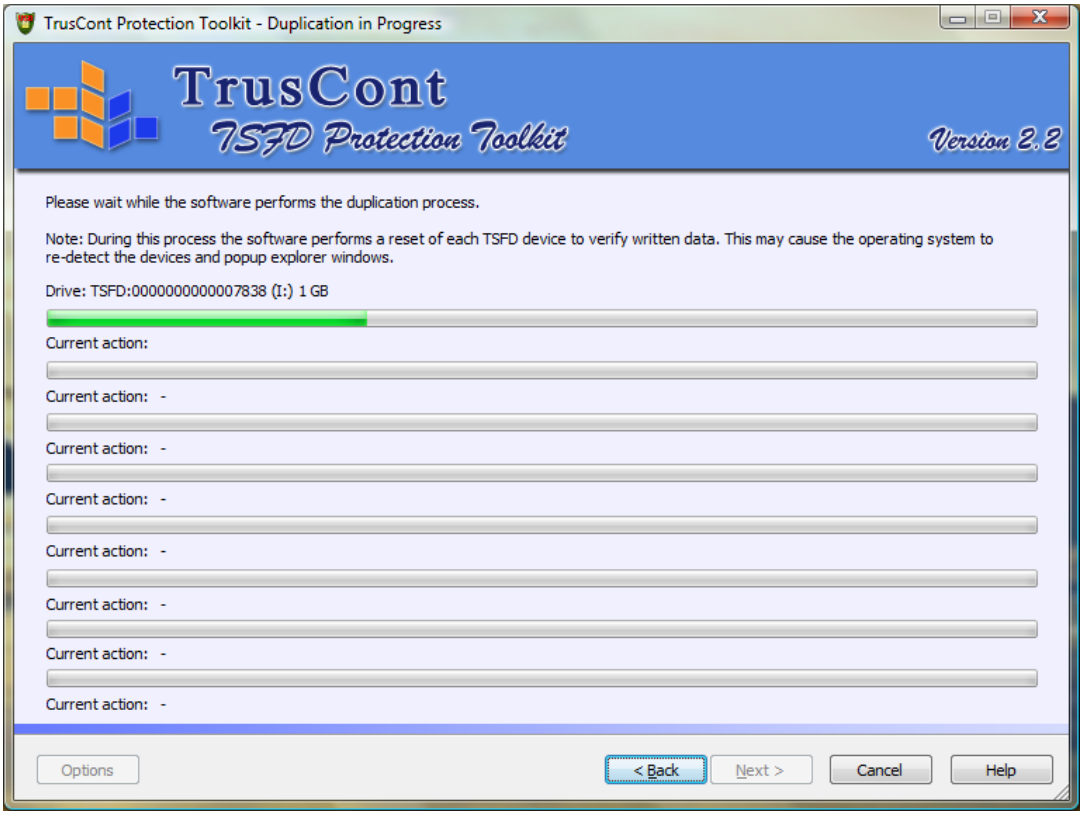
TrusCont Protection Toolkit - Duplication in Progress
TrusCont
TSFD Protection Toolkit
Version 2.2
Please wait while the software performs the duplication process.
Note: During this process the software performs a reset of each TSFD device to verify written data. This may cause the operating system to re-detect the devices and popup explorer windows.
Drive: TSFD:0000000000007838 (I:) 1 GB
Current action:
Current action: -
Current action: -
Current action: -
Current action: -
Current action: -
Current action: -
Current action: -
Options
< Back
Next >
Cancel
Help

Figure 39: TSFD Recording Process

5.5 Using the Toolkit's Project File Association

Installing the Toolkit on your computer also associates the TrusCont TSFD Project File types with the Toolkit. This allows you to open a saved project by simply double-clicking it. When double clicking a saved project, the Toolkit launches and opens your project. The Toolkit skips directly to the 'Edit Project' page allowing you to modify it before proceeding with the duplication process. When double clicking an image, the Toolkit automatically opens it for duplication and skips directly to the 'Select Target' page.

6. Advanced Licensing and Publishing Options

In addition to protecting your files, the TSFD Protection Toolkit also enables the following advanced licensing tasks:

1. **License production to 3rd parties** – Using the Toolkit you can protect and duplicate your files on TSFDs using your own PC. However, sometimes publishers choose to outsource the production to service providers (e.g. duplication houses). The TSFD Protection Toolkit allows you to control the number of copies a service provider will be able to duplicate from an image that you create.
2. **Control updates sent to customers** – The Toolkit allows you to create update files for TSFDs that were already sent to end users. Advanced license control can help you control which customers can apply the updates.

The process includes 3 main steps (see detailed instructions on the following subsections):

1. Create a custom license type using the TrusCont License Management System.
2. Create a portable image (*.tcpi, or *.exe for updates) file using the Toolkit and set it to require your custom license type
3. Transfer custom licenses to a service provider in order to control production, or send a license code to an end user to allow an update.

6.1 Creating a Custom License Type

TrusCont License Management System manages licensing of all TrusCont products. For example, it controls all the production, and use of TrusCont Enhanced DVD-R, as well as the production of TSFDs worldwide.

TrusCont also allows its publishing customers to license the production of their own products to service providers. Customers can create their own custom license types. Custom license types can also be used to control updates of TSFDs that were already sent to end users.

6.1.1 Entering the License Management System

Go to the URL: http://license.truscont.com and use your TrusCont username (email) and password to login.

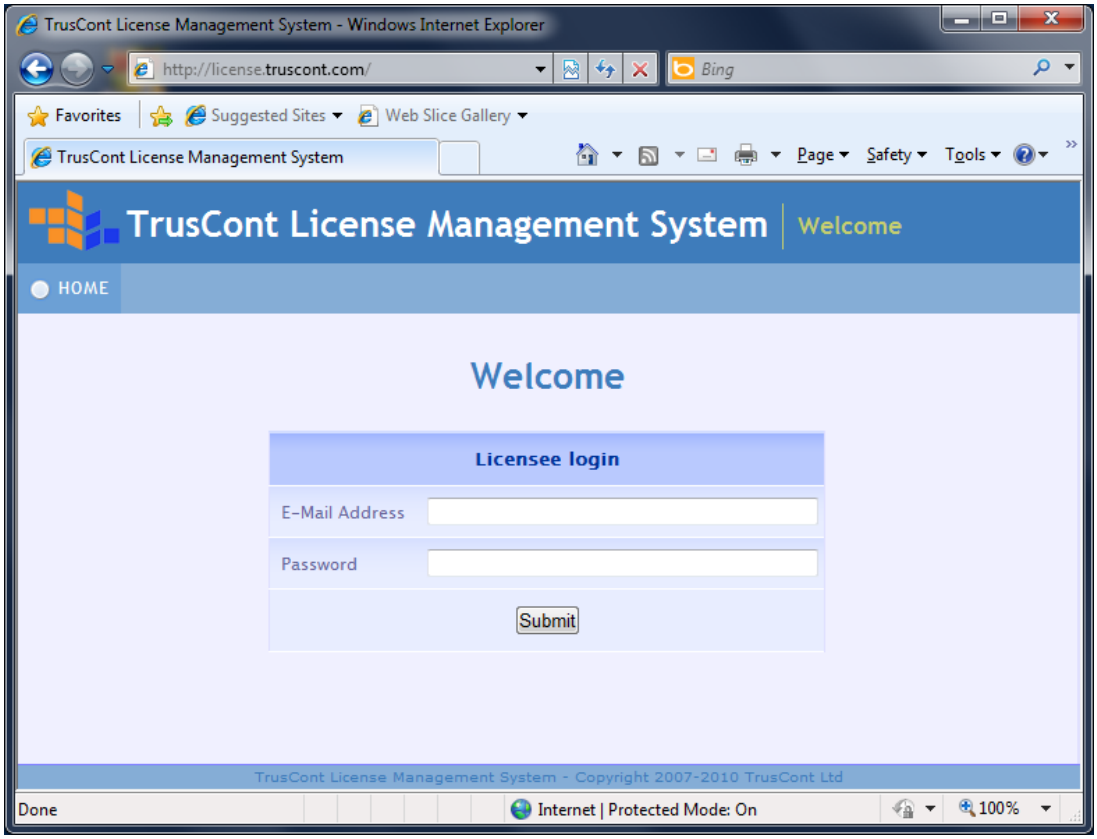

Figure 40: License Management System Login Page

6.1.2 Checking Account Balance

Creating a custom license type requires a "TrusCont Update License". TrusCont Update License is a generic license type used to create custom license types. Each TrusCont Update License can be redeemed to a custom license type that you can define. Use these instructions to check your TrusCont Update License:

1. Go to the 'Home' tab
2. Click 'My Accounts' to view a list of all your license accounts. Most customers have only a single license account.

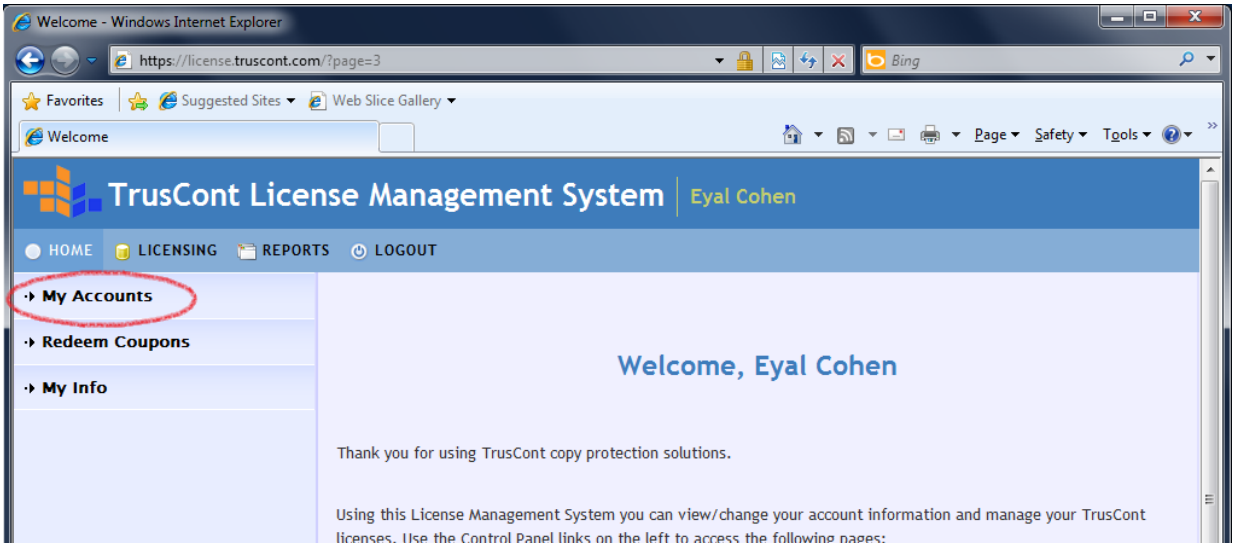

Figure 41: Home Page of the License Management System

3. Click your account number. If you don't have a license account yet, contact your TrusCont representative in order to create an account and purchase TrusCont Update Licenses.
4. If you have more than one license account, click the number of your primary account.

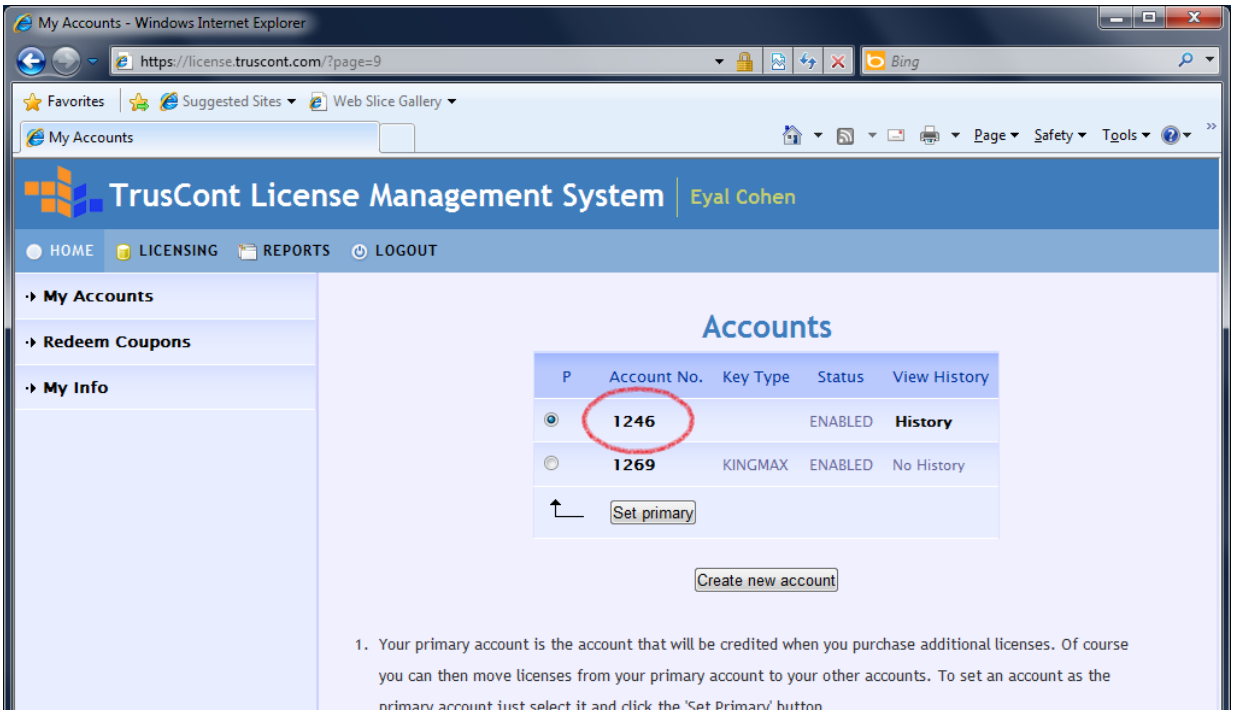

Figure 42: List of License Accounts

5. Check your account balance for TrusCont Update Licenses. If you don't have TrusCont Update Licenses contact your TrusCont representative to purchase the number of licenses you need.

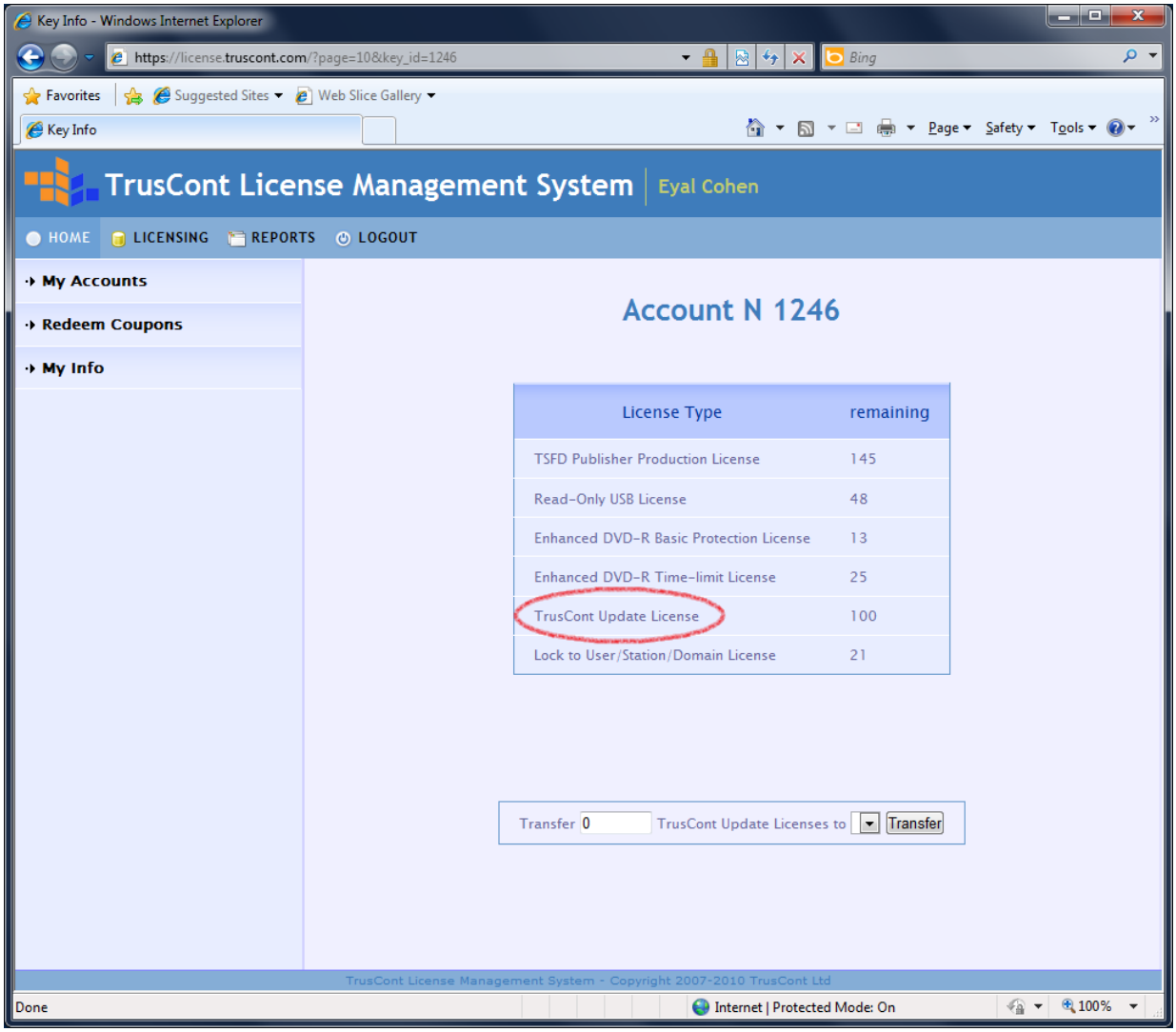

Figure 43: Account Balance

6.1.3 Creating a New License Type

1. Go to the 'Licensing' tab. If you don't have this tab on your account then contact your TrusCont representative in order to get permission for this tab.
2. Click the 'License Types' option.
3. Enter a name for your new license type. Choose a name that you can easily associate with your product in the future. For example, your product name and version.
4. Under 'License Quantity' enter the number of TrusCont Update Licenses that you wish to redeem to your new license type.
5. Click 'Create New License'

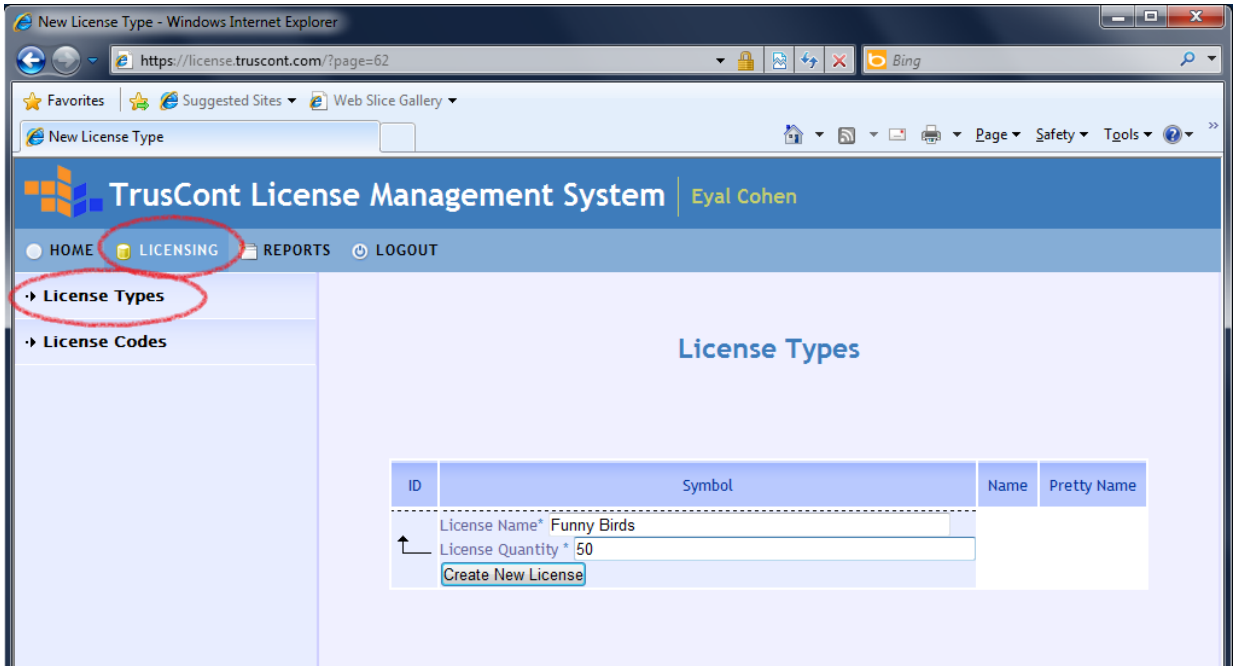

Figure 44: Creating a New License Type

6. You can now see your new license type on the list.

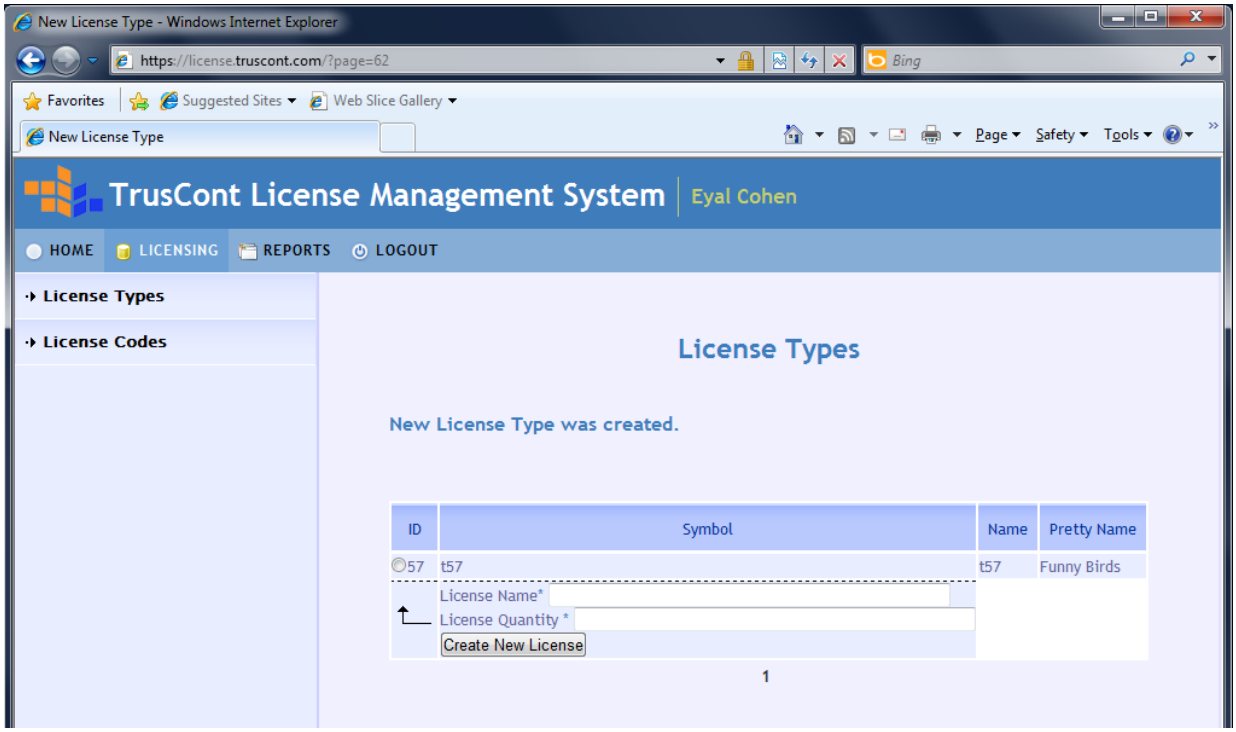

Figure 45: List of Custom License Types

7. You can also see the balance of your new custom license type on your account balance. Go to 'Home'->'My Accounts', and click the account number to check your balance. In this example 50

TrusCont Update Licenses were redeemed to a new license type named 'Funny Birds'. The previous balance of TrusCont Update Licenses was 100, now it is 50.

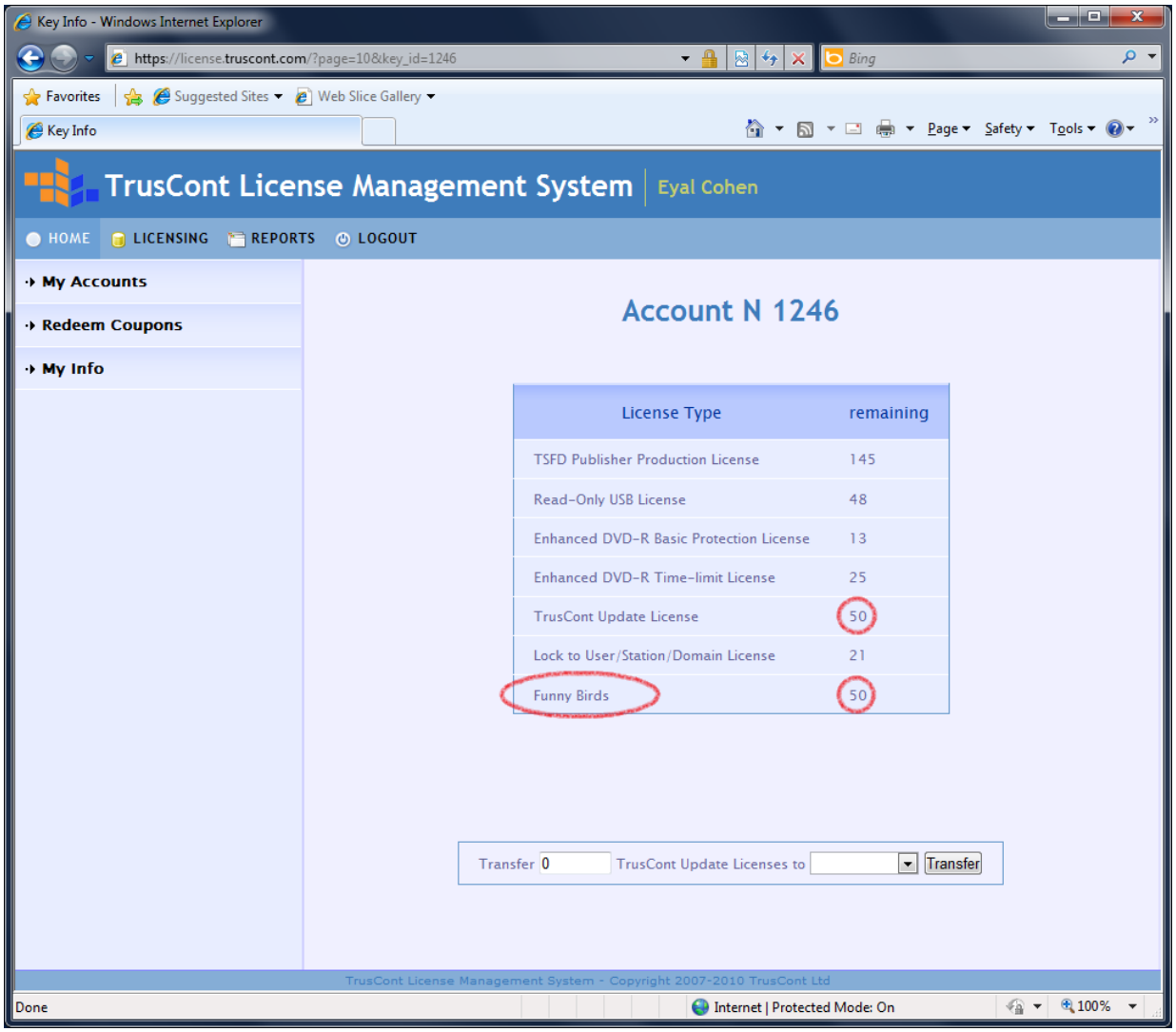

Figure 46: Checking the Balance of Custom License Types

6.1.4 Allocating Additional Custom Licenses

If you wish to redeem additional TrusCont Update Licenses to your custom license type simply use the form at the bottom of the account balance page. Enter the number of licenses you wish to redeem, then specify the target custom license type and click 'transfer'.

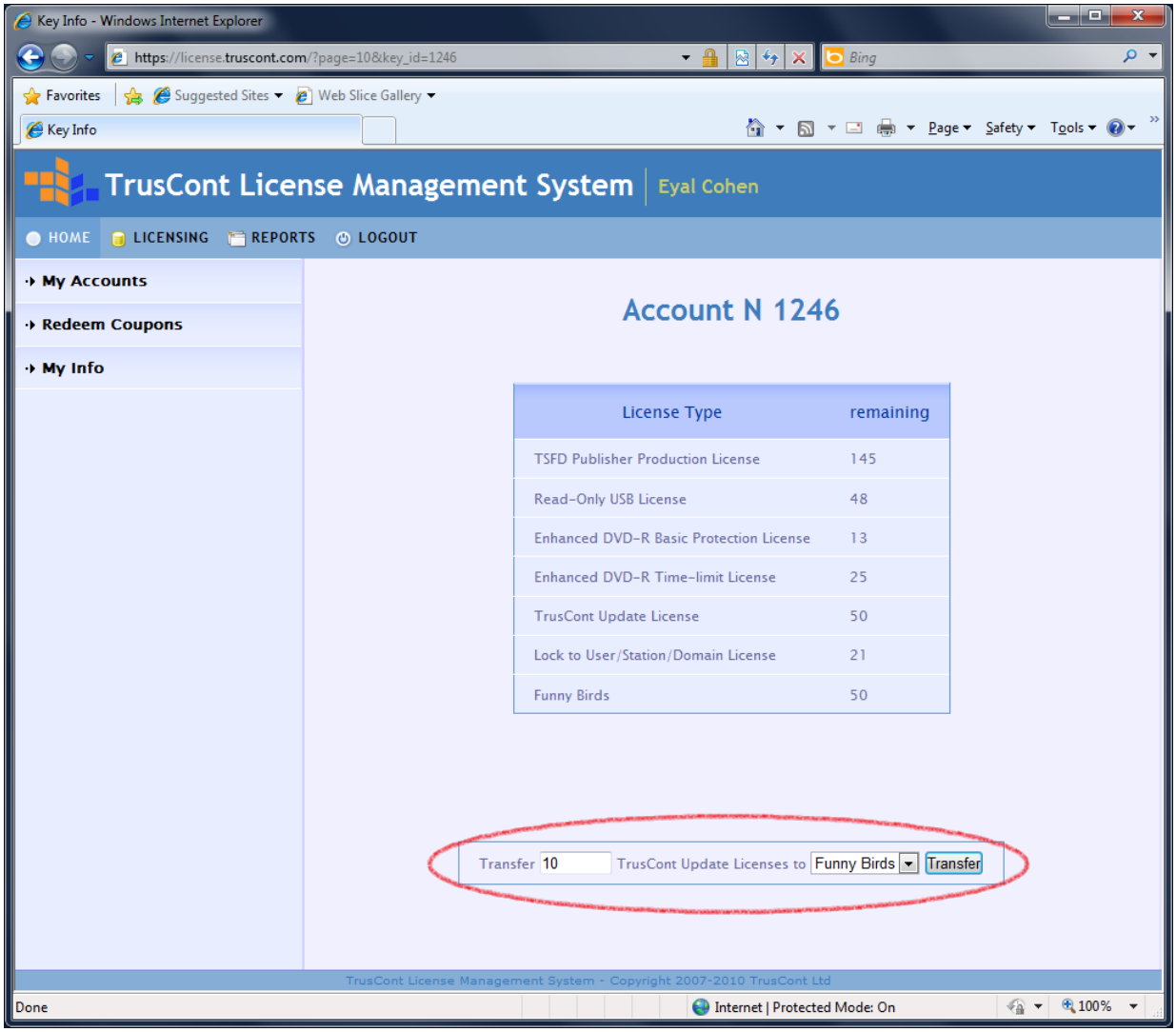

Figure 47: Allocate Additional Custom Licenses

7. Licensing Production to Service Providers

7.1 Creating an Image that Requires a Custom License

In order to create an image that requires a custom license type you will first need to create a custom license type using the TrusCont License Management System. See instructions in section *6.1 Creating a Custom License Type*.

In this example we are creating an image for a product called "Funny Birds". A custom license type named "Funny Birds" was created for the purpose of this example.

Important notes:

- All custom license types are unique. You cannot see custom license types created by other customers unless they specifically transfer their licenses to your account.
- Multiple customers can create custom license types with the same name. However, they will still be different license types and will not be interchangeable in any way.

Instructions for creating the image (for details instructions refer to section *5.2, Creating a New Project*):

1. Open the TSFD Protection Toolkit
2. Create a new project.
3. Add your product files to the project.
4. Set protection options and other settings as required.
5. Set the media title
6. On the select action page select 'Create TrusCont Portable Image (*.tcpi)

Bind the portable image to your custom license type (see figure on next page):

1. Under 'Product Settings' set the 'Product Type' option.
2. The toolkit will ask you for your TrusCont username (email) and password in order to login to your account and retrieve the list of custom license types you have created.
3. Select the custom license type to which you wish to bind your image. In this example the image of our "Funny Birds" product is bound to our "Funny Birds" license type.
4. Click 'Next' and proceed with the image creation (see section *5.2.7 above*)

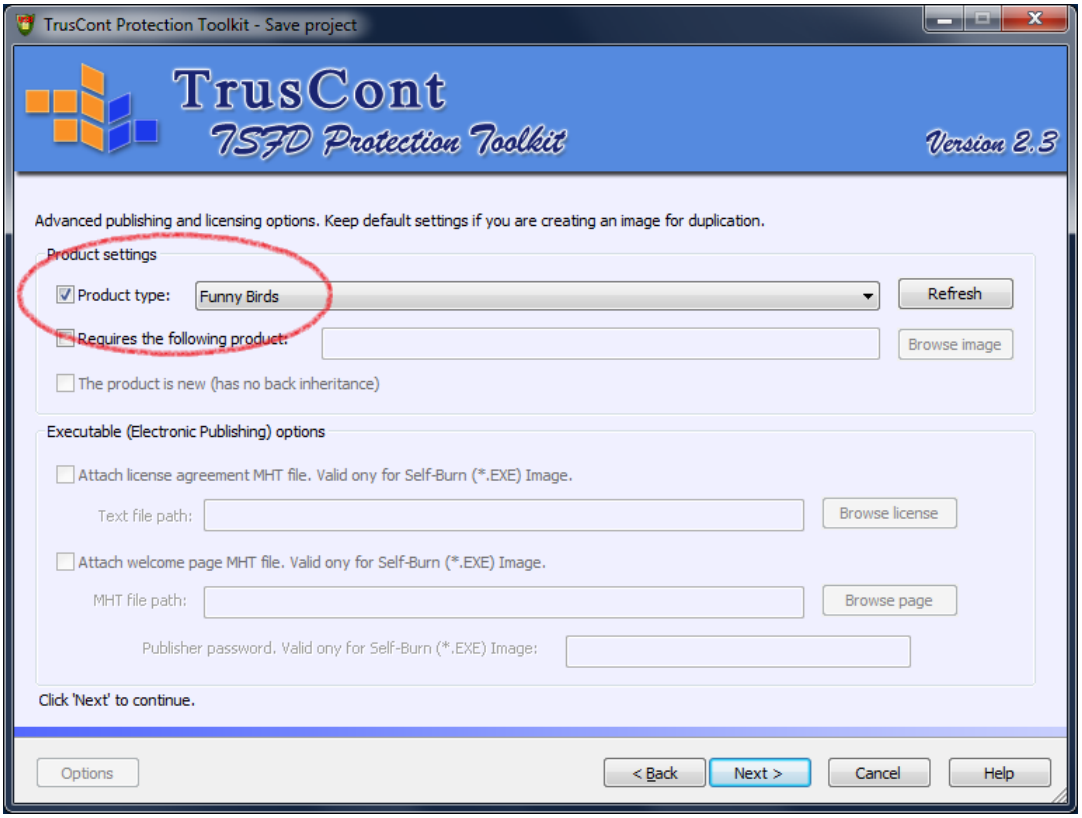
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Funny Birds
Refresh
Requires the following product:
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 48: Crating an Image that Requires a Custom License Type

The image file is now bound to the new "Funny Birds" license type. This means that no one can duplicate this image onto TSFDs without first receiving "Funny Birds" licenses.

7.2 Transferring Custom Licenses to a Service Provider

In order to allow a service provider to duplicate 50 copies of the "Funny Birds" image we need to transfer 50 "Funny Birds" licenses to his account:

1. Ask your service provider for his license account number. Your service provider can check what is his account number on the License Management System under 'My Accounts'.
2. Login to the TrusCont License Management System
3. Go to the 'Licensing' tab.
4. Click the 'Transactions' option
5. Under the 'From' section of the 'Transaction' form:
    a. Verify that your primary account number is selected.
    b. Select the license type that – in this example "Funny Birds"
6. Under the 'To' section of the 'Transaction' form:
    a. Enter the account number of your service provider.
    b. Specify the number of licenses you wish to transfer to your service provider.

c. Optionally enter a comment – this comment will appear in your account history for your reference (accessible via the 'History' link next to your account number under the 'Home'->'My Accounts' page)

d. Click 'Ok'

e. A confirmation page will be displayed. Review the information and confirm to complete the transaction

The service provider will now be able to duplicate only 50 copies of the "Funny Birds" image.

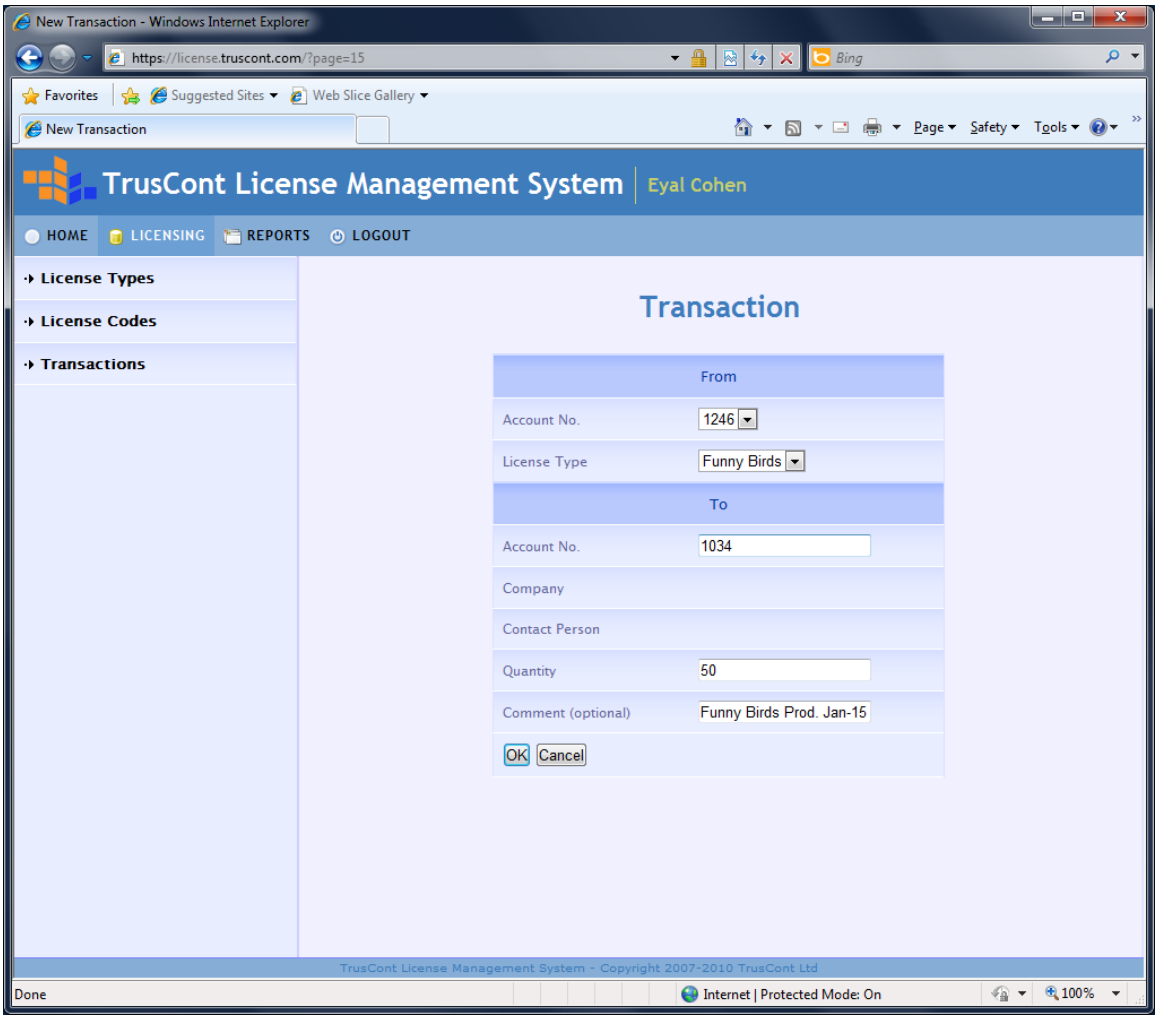

Figure 49: Transferring Custom Licenses to a Service Provider

8. Updating Content on TrusCont Secure Flash Drives

Protected content on TSFDs can be updated, or overwritten unlimited number of times during the 1 year license term of each TSFD.

If you have access to the TSFD you wish to update, you can simply overwrite it with the TSFD Protection Toolkit. However, in many cases content owners wish to update the content of flash drives that were already sent to customers.

8.1 Making a Product Updateable

- Keep the original image of your product
  Create an image file using the TSFD Protection Toolkit and use this image to record all TSFDs you plan to distribute to your customers. Archive the image in a safe place - you will need it in the future whenever you would like to create an update for your specific product.

- Apply publisher passwords to your TSFDs
  Publisher passwords are useful to make sure that only you can update the TSFDs in the future. When you create updates in the future you will need to provide the same password to the TSFD Protection Toolkit. The password will be encoded within the update file. Your customers will never need to know or to enter this password. Only updates that are protected with the same password can be applied to your TSFDs. No one else will be able to publish updates for your TSFDs, or overwrite your content in any way.

8.2 Creating TSFD Updates

Using the TSFD Protection Toolkit you can create update files. The update file is actually a single EXE file that contains the updated content. Your customers simply have to double click it and confirm the update process. The update file will automatically overwrite the customer's TSFD with the updated content.

There are several types of updates that can be created:

- **Generic updates** – Generic updates are updates that don't require the customer to have a specific product on his TSFD, or a specific license to apply the update. It is actually a method for completely overwriting the TSFD with new content.

- **Updates for a specific product** – These are updates that can be applied to TSFDs that already contain a specific product. You must have the original image that you have recorded on your customers' TSFDs in order to create such an update.
- **Updates that require a license (selective update for specific customers)** – It is also possible to create updates that require a license code. When a customer will try to apply the update to his TSFD the update will ask him for a license code.

- **Updates that create a new product** – These are updates that completely erase the target TSFD and record on it a new product.

8.3 Creating an Update File

Update files actually completely overwrite the end users' TSFDs with the new content that you specify. The process is similar to creating a new image file:

1. Open the TSFD Protection Toolkit
2. Create a new project
3. Add files to your project. Add all the files you wish to be present on the target TSFD following the update process. The update process will completely overwrite and delete all previous files on the target TSFD
4. Set protection options and other settings as required.
5. Set the media title
6. On the select action page select 'Create TrusCont Portable Image (*.exe)

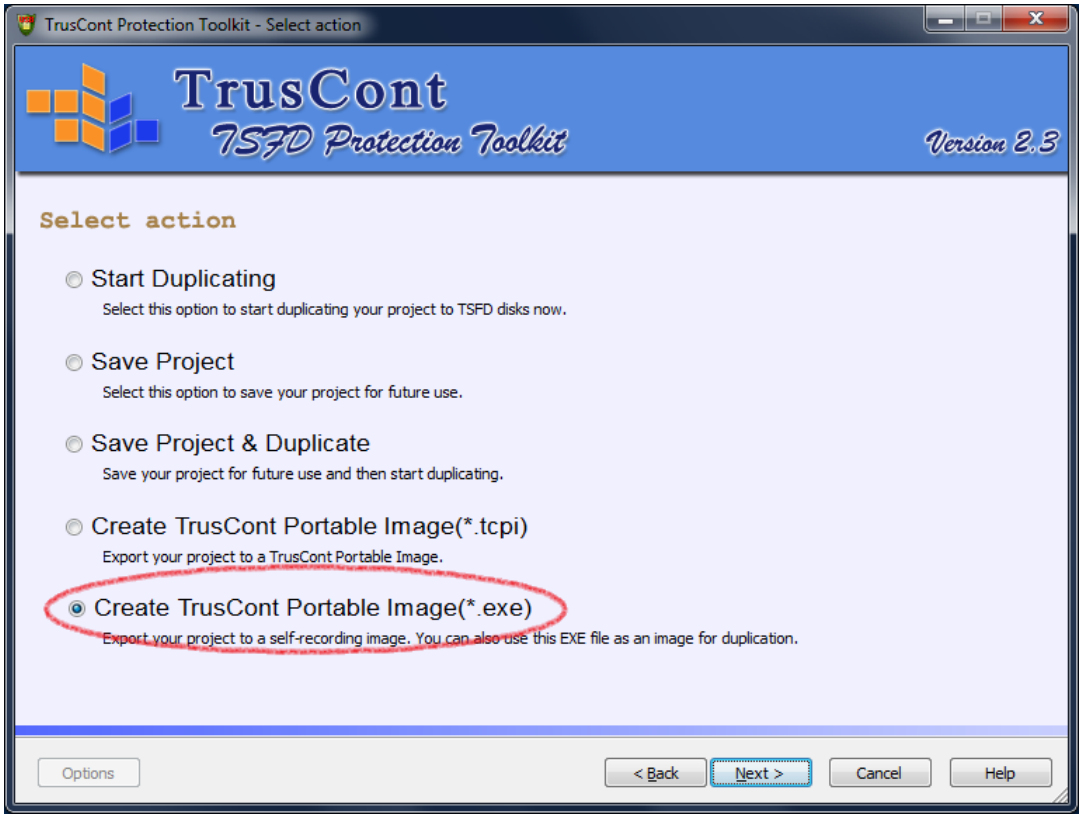
TrusCont Protection Toolkit - Select action
TrusCont
TSFD Protection Toolkit
Version 2.3
Select action
Start Duplicating
Select this option to start duplicating your project to TSFD disks now.
Save Project
Select this option to save your project for future use.
Save Project & Duplicate
Save your project for future use and then start duplicating.
Create TrusCont Portable Image(*.tcpi)
Export your project to a TrusCont Portable Image.
Create TrusCont Portable Image(*.exe)
Export your project to a self-recording image. You can also use this EXE file as an image for duplication.
Options
< Back
Next >
Cancel
Help

Figure 50: Creating an Update File

Set the image settings according to the update type you wish to generate (see following sections for instructions)

8.3.1 Creating Generic Updates

To create a generic update that can be applied to any TSFD clear all options on the 'Advanced Publishing and Licensing' page.

Important notes:

1. The update file cannot be applied to target TSFDs that are protected with a publisher password, unless you specify the same password under the 'Publisher password' option as show in the figure below.
2. If the update file includes a publisher password and it is applied to TSFDs that are not protected with a publisher password, the password will be set on the TSFDs and any future updates will have to include the same password in order to update the same TSFDs.

Click 'Next' and proceed with the image creation (see section *5.2.7 above*)

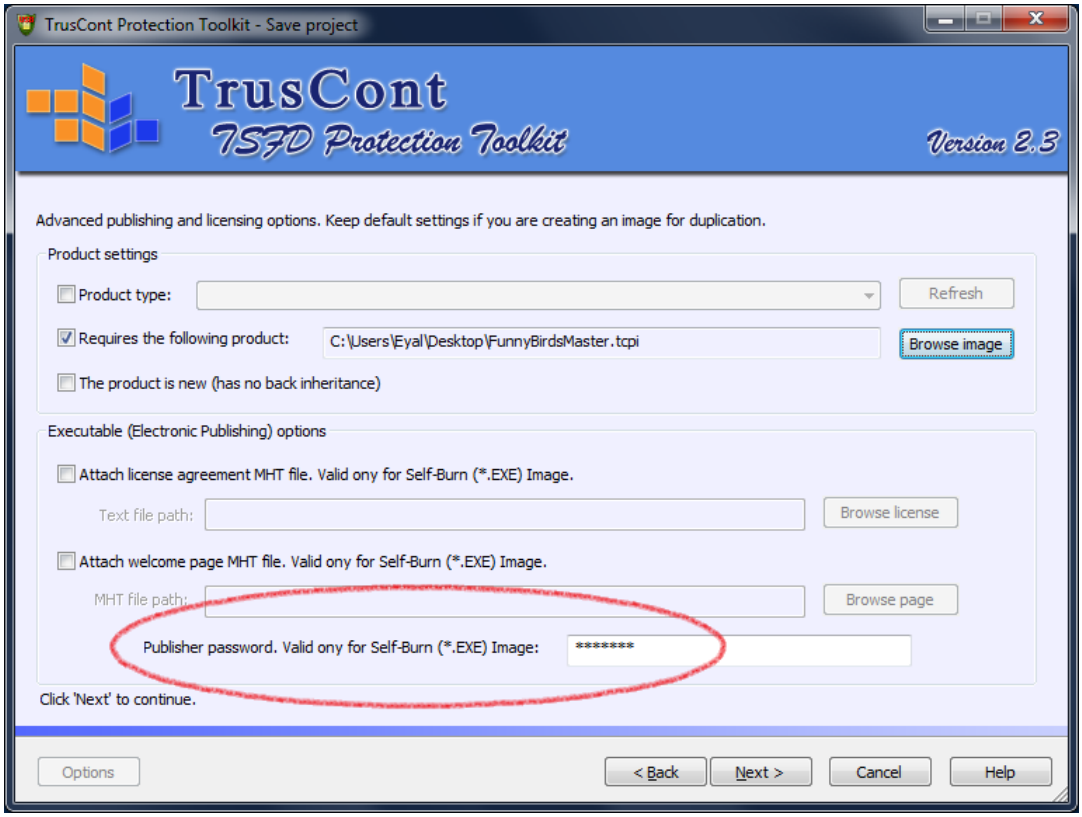
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Refresh
Requires the following product:
C:\Users\Eyal\Desktop\FunnyBirdsMaster.tcpi
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
****
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 51: Creating Generic Updates

8.3.2 Creating Updates for TSFDs Containing a Specific Product

In order to create an update file that can be applied only to TSFDs that contain a specific product:

1. Check the 'Requires the following product' option
2. Click the 'Browse image' button and select the image file of the product that shall be required. This is the original image that you (or your service provider) recorded on the TSFDs that you wish to update.
3. If the target TSFDs that you wish to update are protected with a publisher password you must specify it under the 'Publisher password' option.
4. Click 'Next' and proceed with the image creation (see section *5.2.7 above*)

Important note: The update can be applied also to target TSFDs that were already updated with previous updates provided that all previous updates required the same product, and none of them was set to create a new product (i.e. the target TSFD still includes the encoding of the original product – see section *8.3.4 Updates that Create a New Product*).

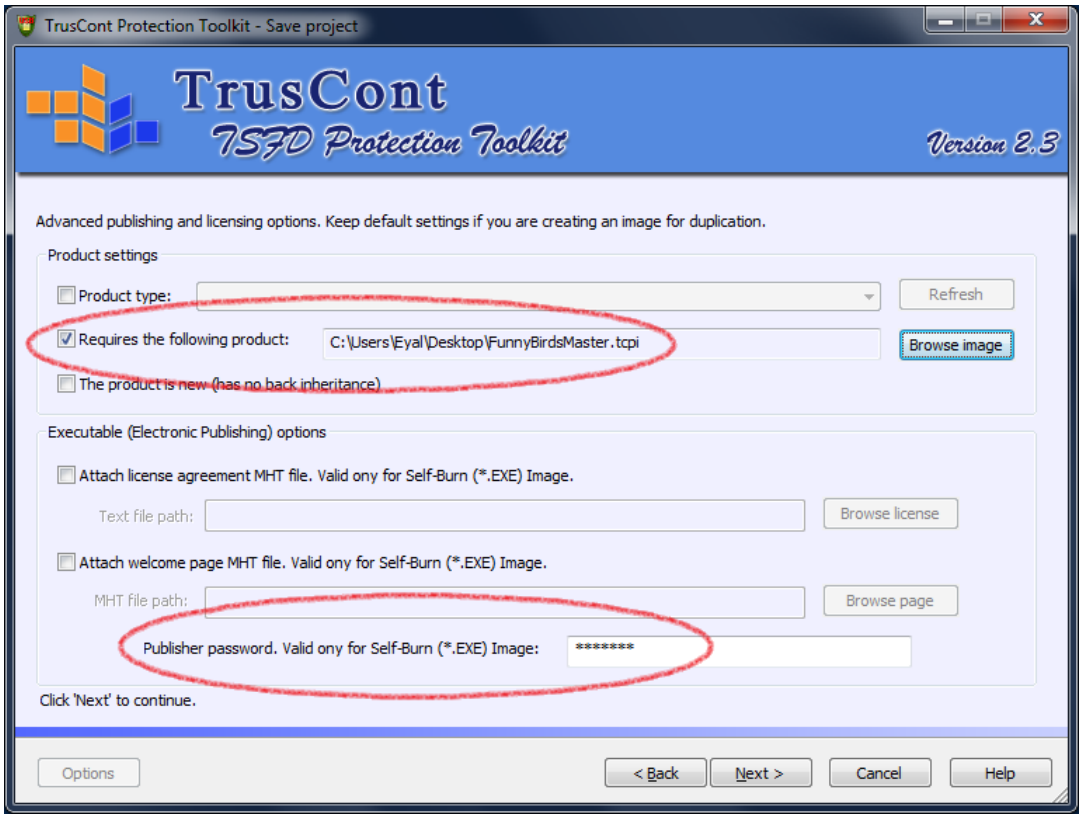
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Refresh
Requires the following product:
C:\Users\Eyal\Desktop\FunnyBirdsMaster.tcpi
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
****
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 52: Creating an Update for TSFDs Containing a Specific Product

8.3.3 Updates that require a license

You can also create updates that can be applied only with a special license code. This is useful when you want to allow only specific customers to apply the update, rather than creating an update file that can be used by all of your customers.

8.3.3.1 Creating a Custom License Type

You will first need to create a new custom license type. For the purpose of this example, a new license type was created with the name "Funny Birds Update 1". On the account balance it is now possible to see the "Funny Birds" license that was used to control the original production, and the "Funny Birds Update 1" that is going to be used for controlling the update.

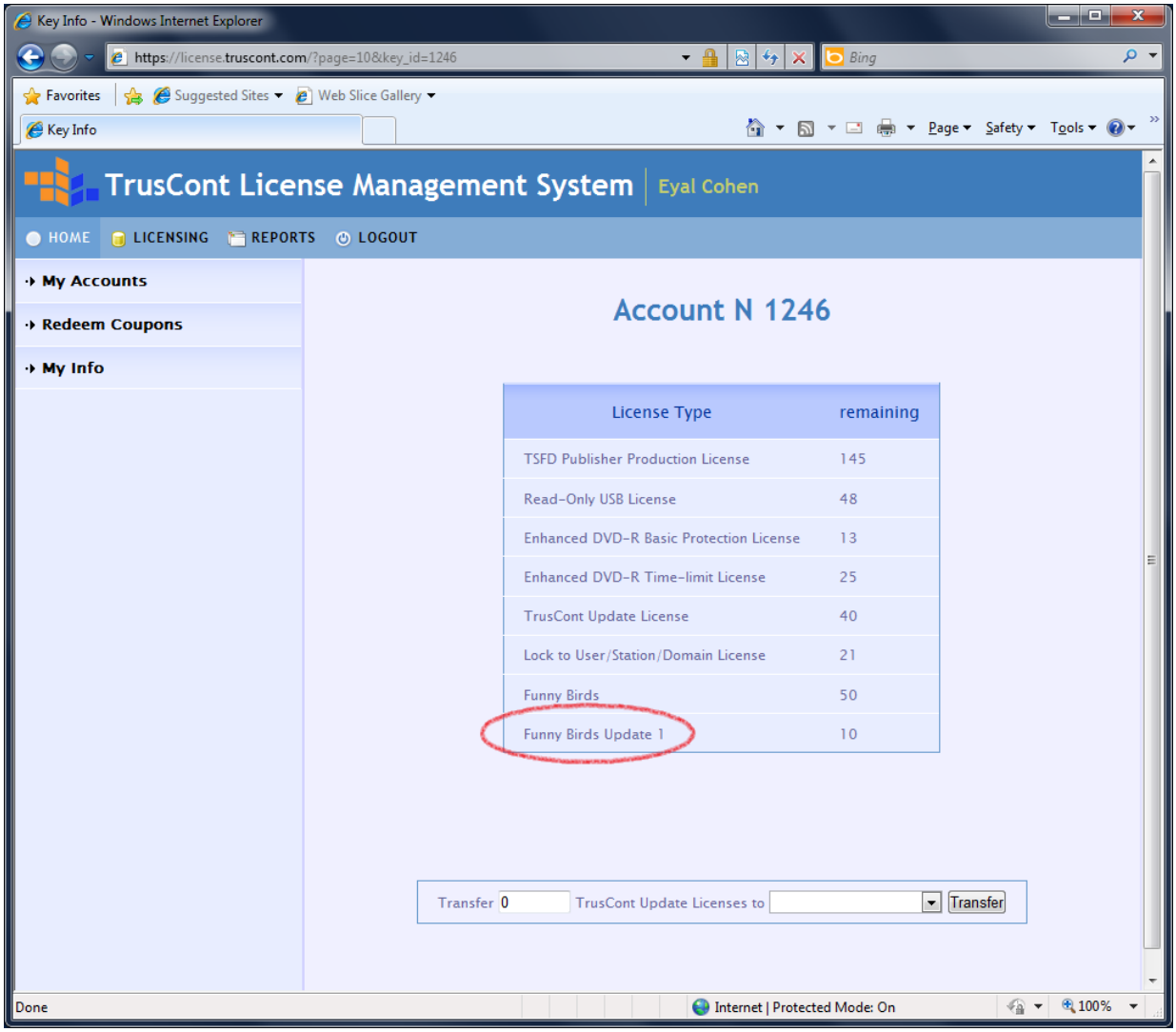

Figure 53: Account Balance with Multiple Custom License Types

8.3.3.2 Creating the Image

Set the following options on the 'Advanced Publishing and Licensing' page:

1. Check the 'Product Type' option, enter your email and password when prompted, and then select the license type that your update shall require. In this example – "Funny Birds Update 1"
2. Check the 'Requires the following product' option, then click 'browse image' and specify the original image that you have recorded on the target TSFDs that you wish to update. In this example – the original image of the "Funny Birds" image.
3. If the target TSFDs are protected with a publisher password you must specify the same password under the 'Publisher password' option.
4. Click 'Next' and proceed with the image creation (see section *5.2.7 above*)

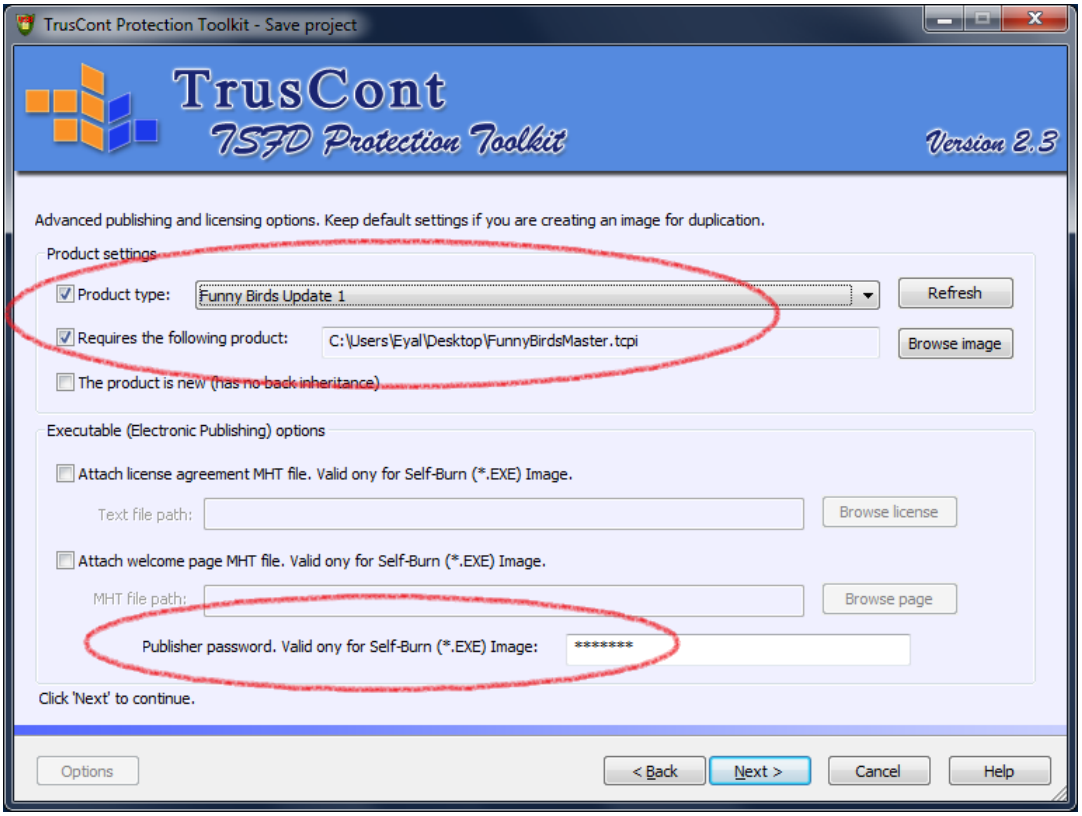
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Funny Birds Update 1
Refresh
Requires the following product:
C:\Users\Eyal\Desktop\FunnyBirdsMaster.tcpi
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
****
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 54: Creating an Update that Requires a License

8.3.3.3 Generating License Code for End Users

The update file in the above example requires end users to have a license code in order to apply it. To create license code for end users:

1. Login to TrusCont License Management System.
2. Go to the 'Licensing' tab.

3. Click the 'License Code' option.
4. Click 'Create New Code(s)'.

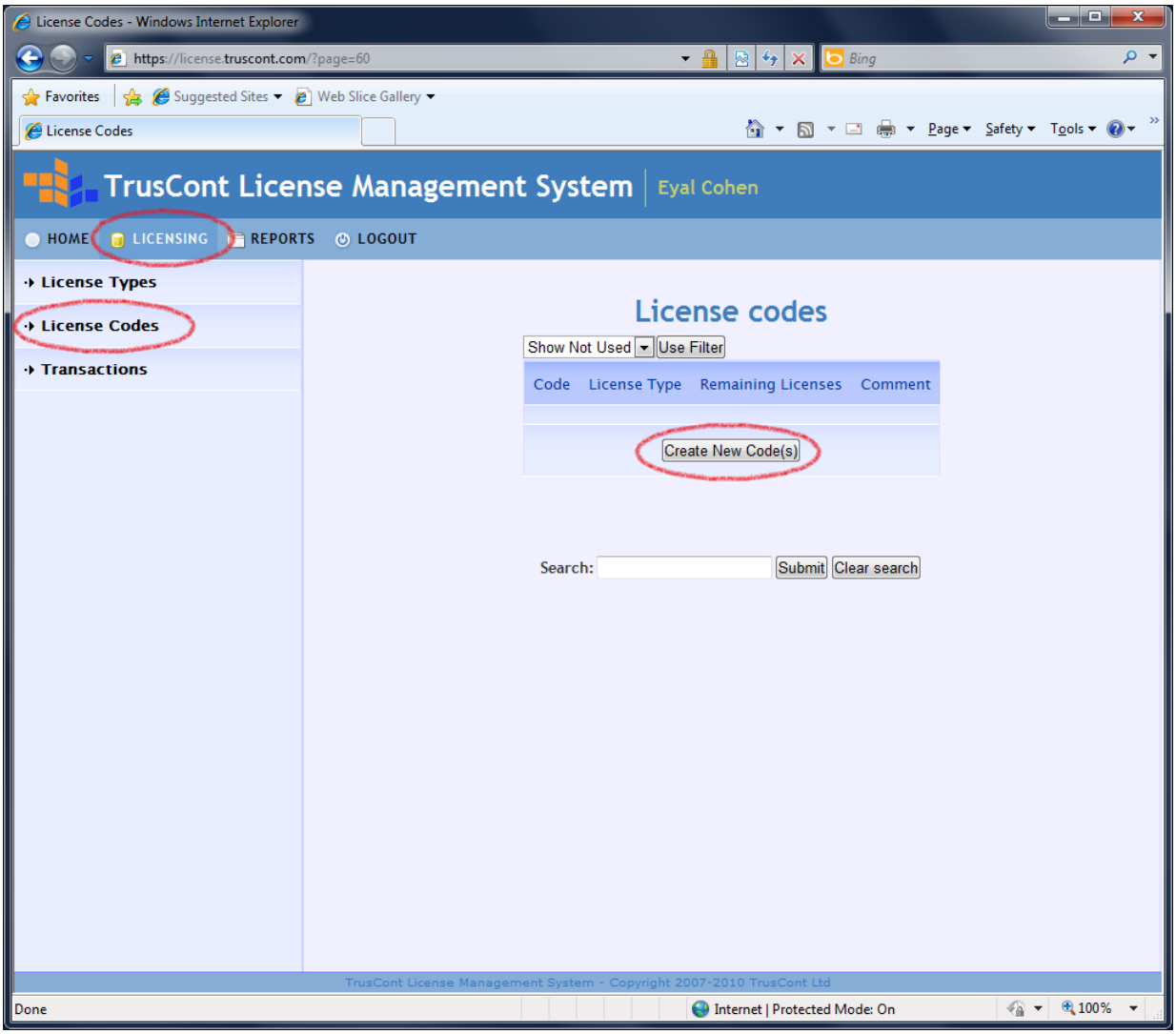

Figure 55: Creating a License Code

The 'Create License Code(s)' form will appear:

1. Specify the license type that you wish to assign to the code (e.g. "Funny Birds Update 1"). It must be the same license type that is required by the update file.
2. Specify the number of licenses you wish to assign to the code. The number of licenses determines the number of times the specific license code can be used to apply the update. In other words – it is the number of TSFDs the specific code can be used to update. Typically each user should get one code that has one license assigned to it. However, if you have a customer that has more than one TSFD that needs to be updated you can set the quantity as required.

3. Optionally enter a comment for your code. This can be your customer name for example. You can see this comment next to the specific code on the codes list under the 'Licensing'->'License codes' page.
4. Enter the number of codes you wish to create. This is useful if you wish to create multiple codes. Each of the codes will be assigned the license types and quantities that you specify.
5. Click 'Ok' to create the code.

Note: It is possible to assign more than one license type to each code.

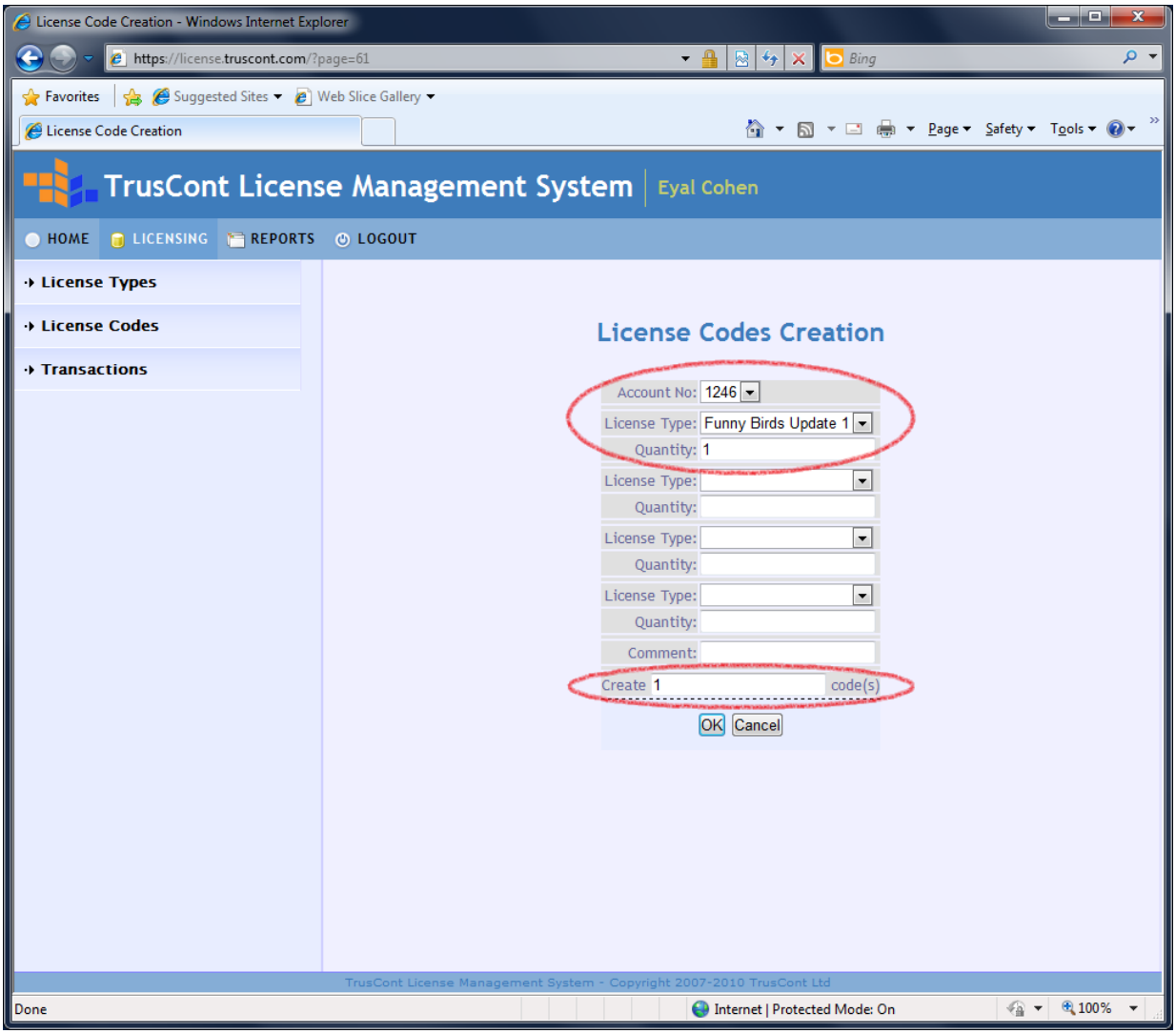

Figure 56: The 'Create License Code' Form

You can see the list of codes you have created on the 'Licensing'->'License Codes' page. By default the License Management System displays the codes that were not used yet. Next to each code you can see the comment that you may have added to the code, and the number of remaining licenses

assigned to the code. To view the codes that were already used, change the filter above the list to 'Show used' and the click the 'Use Filter' button.

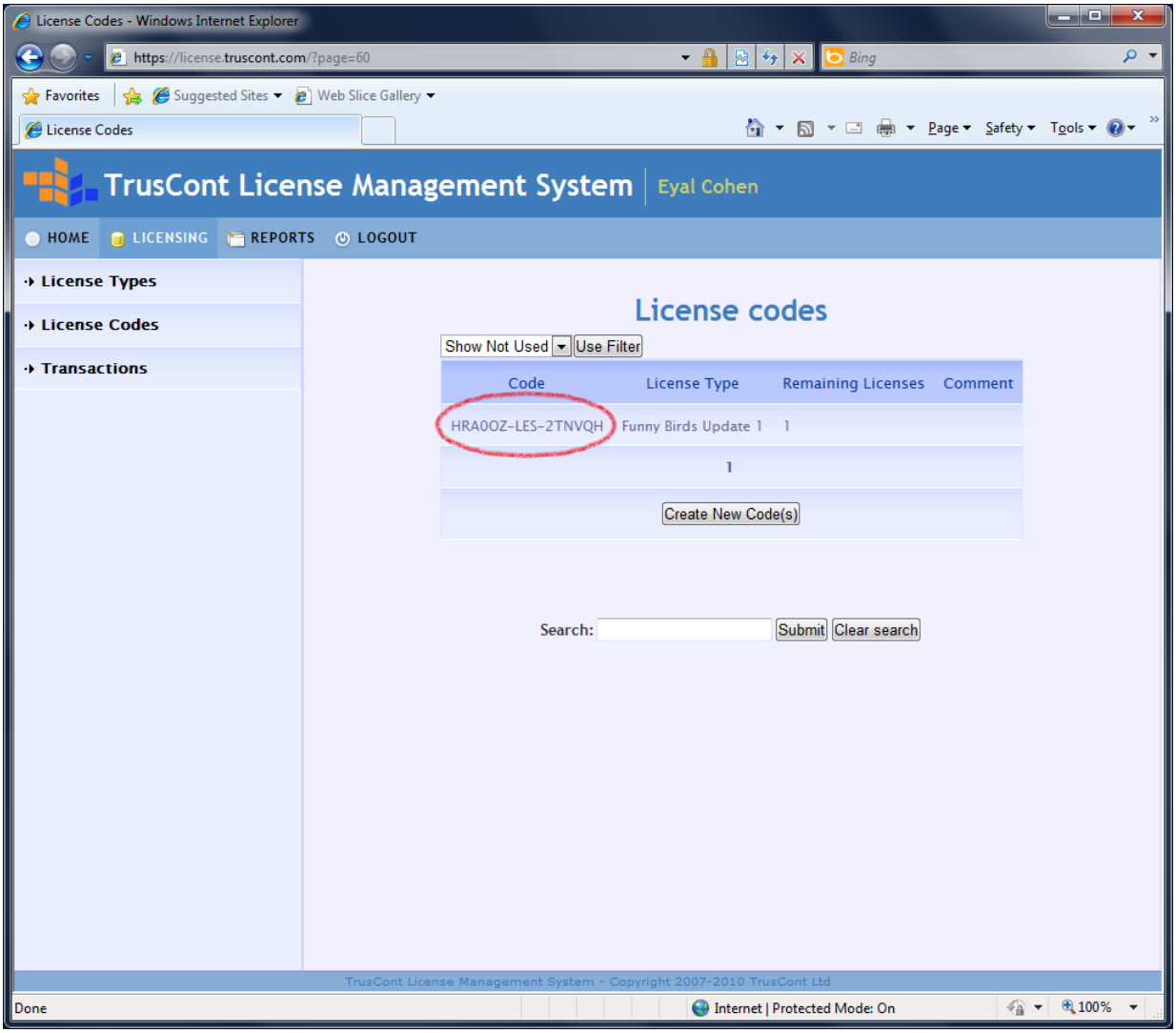

Figure 57: License Codes List

8.3.3.4 Creating Multiple Updates for the Same Product

It is possible to update the same product multiple times. For example, it is possible to create also a second update file for our "Funny Birds" product and set it to require a second license type – e.g. "Funny Birds Update 2". If all updates require the same original product ("Funny Birds"), end users can apply any of the updates even if a previous update was not applied. It is even possible to apply a previous update after applying the latest one – effectively rolling back the product to an earlier version. This is possible even if the updates do not require a license code (only require a specific product).

8.3.4 Updates that Create a New Product

If you are going to send an update to end users that completely replaces the original product with a new product, you probably want to prevent future updates of the new product from being applied to TSFDs that will still contain the first product.

For example, we can create an update that replaces our "Funny Birds" product with a "Parrots Album" product. At some time in the future we may have some customers that have purchased and applied our new "Parrots Album" product on their TSFDs, and other customers that still have our old "Funny Birds" product on their TSFDs. If we then create an update for our "Parrots Album" product (e.g. "Parrots Album Update 1") we wouldn't want the customers that still use the "Funny Birds" product to be able to apply on their TSFDs.

To create an update that completely replaces an existing product with a new product, first create a new license type for the new product – e.g. "Parrots Album".

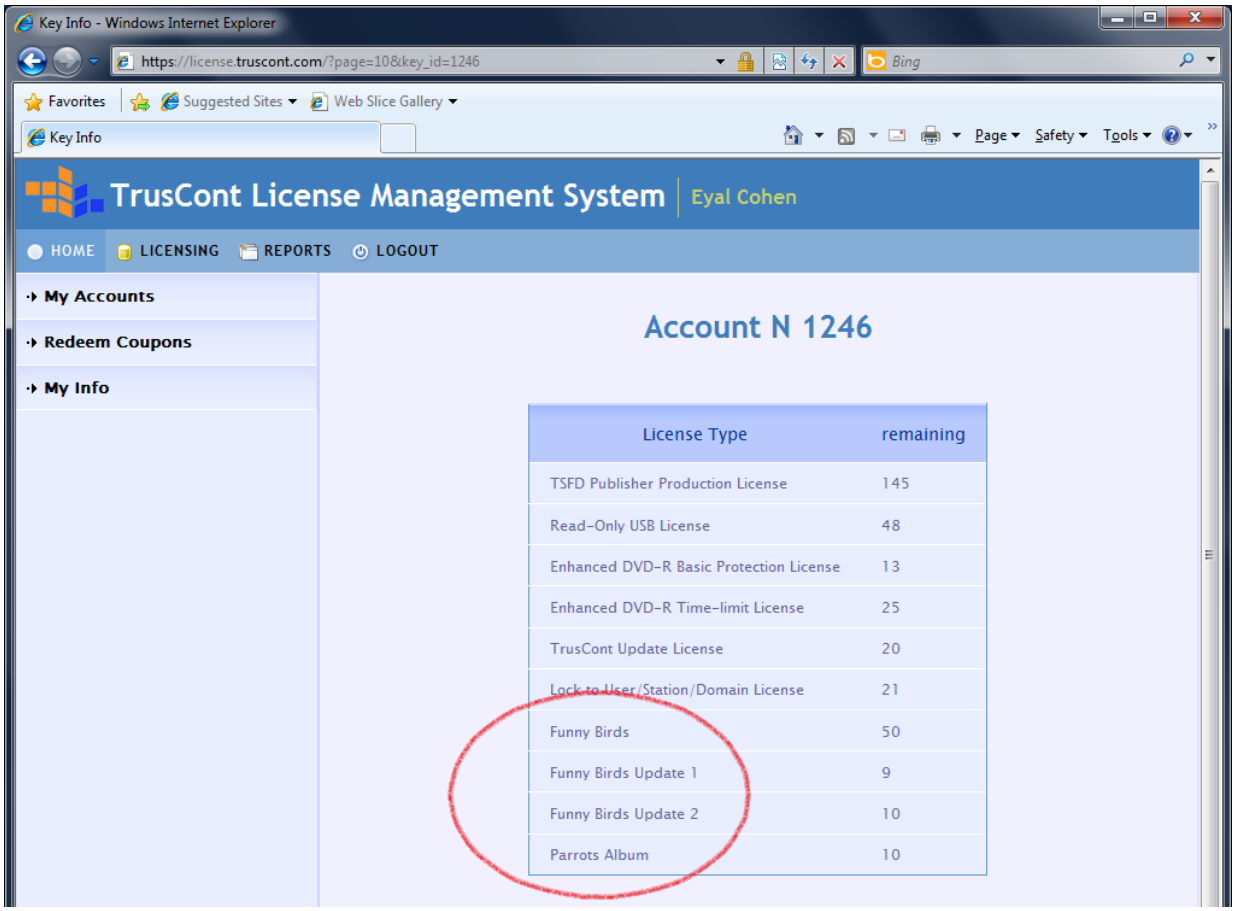

Figure 58: License Types Balance

Set the following options on the 'Advanced Publishing and Licensing' page:

1. Check the 'Product Type' option, enter your email and password when prompted, and then select the license type that your update shall require. In this example – "Parrots Album"
2. Check the 'Requires the following product' option, then click 'browse image' and specify the original image that you have recorded on the target TSFDs that you wish to update. In this example – the original image of the "Funny Birds" image.
3. Check the 'The product is new' option.
4. If the target TSFDs are protected with a publisher password you must specify the same password under the 'Publisher password' option.
5. Click 'Next' and proceed with the image creation (see section *5.2.7 above*)

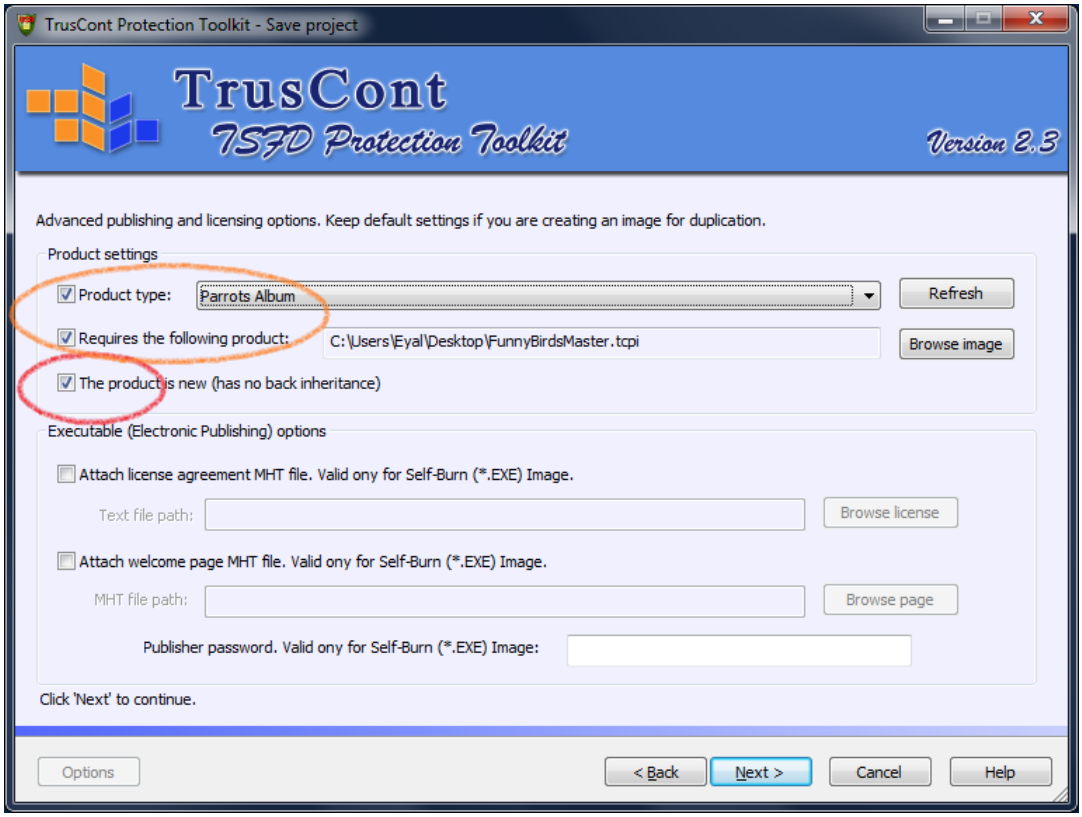
TrusCont Protection Toolkit - Save project
TrusCont
TSFD Protection Toolkit
Version 2.3
Advanced publishing and licensing options. Keep default settings if you are creating an image for duplication.
Product settings
Product type:
Parrots Album
Refresh
Requires the following product:
C:\Users\Eyal\Desktop\FunnyBirdsMaster.tcpi
Browse image
The product is new (has no back inheritance)
Executable (Electronic Publishing) options
Attach license agreement MHT file. Valid ony for Self-Burn (*.EXE) Image.
Text file path:
Browse license
Attach welcome page MHT file. Valid ony for Self-Burn (*.EXE) Image.
MHT file path:
Browse page
Publisher password. Valid ony for Self-Burn (*.EXE) Image:
Click 'Next' to continue.
Options
< Back
Next >
Cancel
Help

Figure 59: Creating an Update that Create a New Product

The following table details which updates of our "Funny Birds" / "Parrots Album" various customers can apply based on the current product / update that exists on their TSFD

Update **Existing Product**	"Funny Birds Update 1"	"Funny Birds Update 2"	"Parrots Album"	"Parrots Album Update X"
Original "Funny Birds"	Yes	Yes	Yes	No
"Funny Birds Update 1"	Yes	Yes	Yes	No
"Funny Birds Update 2"	Yes	Yes	Yes	No
"Parrots Album"	No	No	No	Yes
"Parrots Album Update X"	No	No	No	Yes

8.4 Adding a Welcome Page and a License Agreement

The Toolkit allows you to add a welcome page that will be displayed when customers run the update file. In addition you can add a license agreement that will be displayed after the welcome page and will require end users to accept it in order to apply the update.

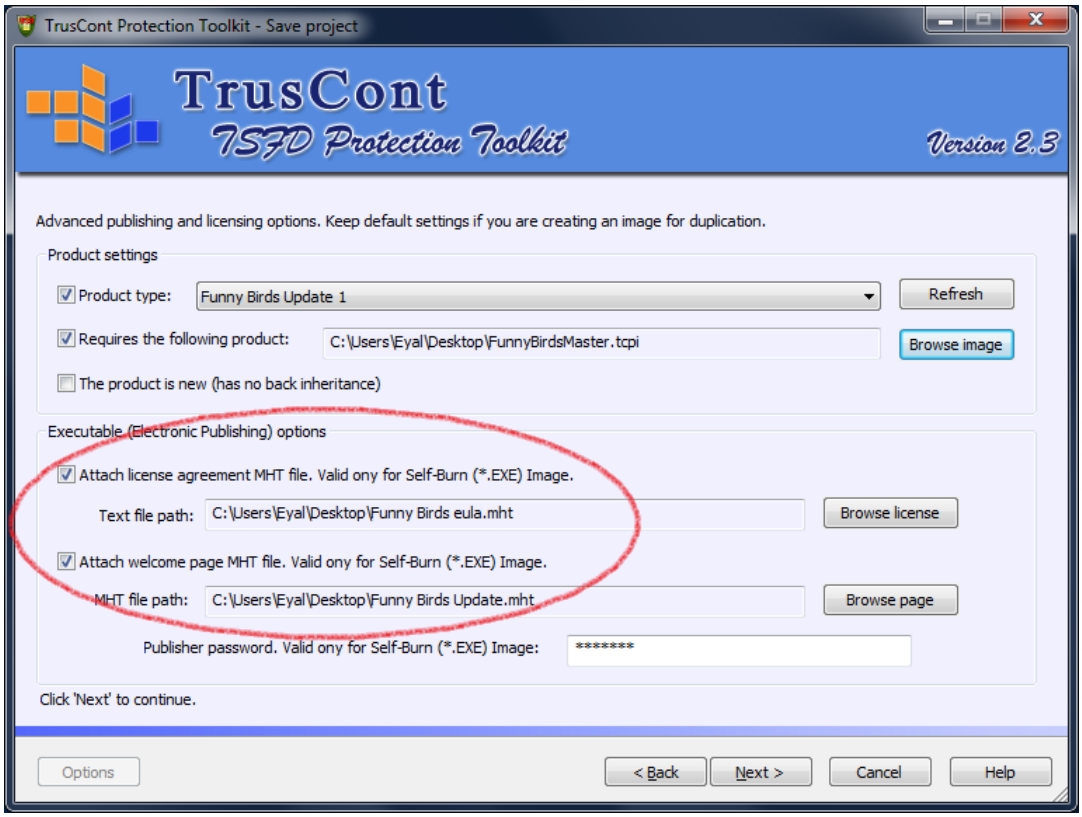

Figure 60: Adding a Welcome Page and a License Agreement

The welcome page and license agreement need to be in a single web page format (MHT file). MHT files can be created using Microsoft Word. Create your documents then select 'Save As' and choose 'Save as type: Single web page (*.mht; *.mhtl)'

On the 'Advanced Publishing and Licensing' page:

1. Check the 'Attach a license agreement…'
2. Click the 'Browse license' button and select the license agreement MHT file
3. Check the 'Attach a welcome page…'
4. Click the 'Browse page' button and select the welcome page MHT file

8.5 Applying an Update

The update file is actually an EXE program file that records the update to the end users' TSFDs. To start the update process the end user simply double clicks the update file.

If you have included a welcome page in your update file, it will be the first page that the end user sees. This is a welcome page sample for our "Funny Birds Update 1":

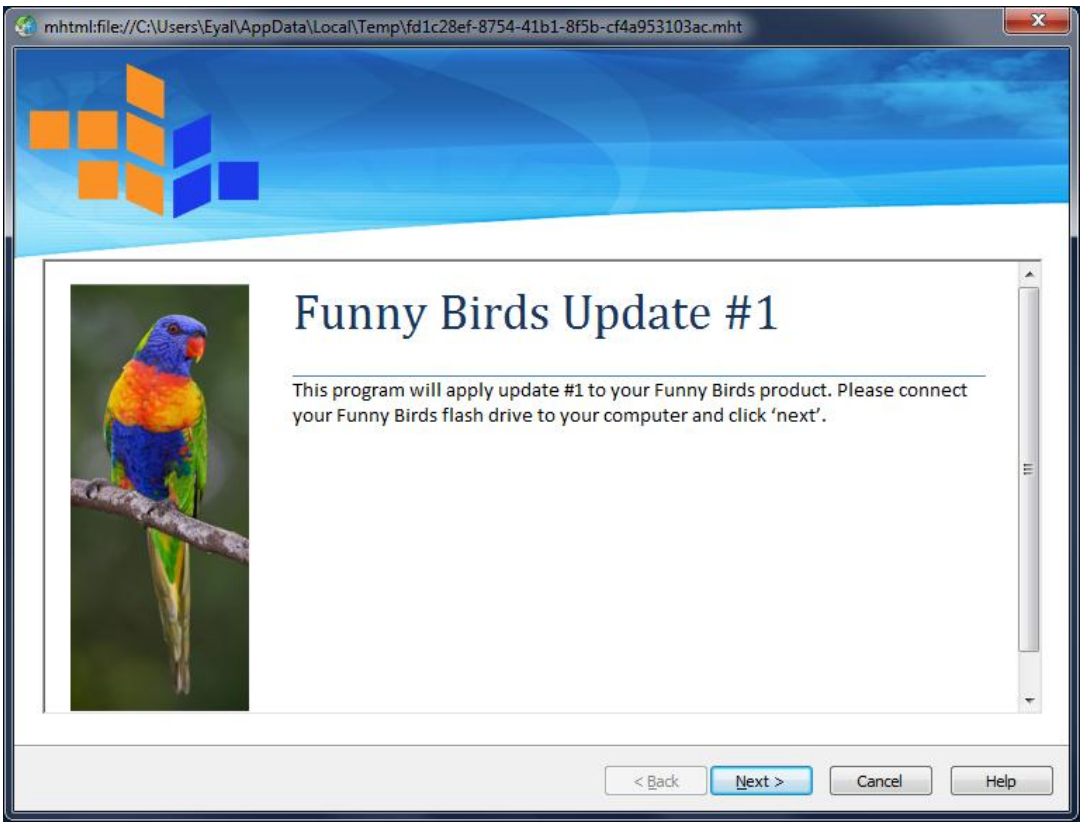
mhtml:file://C:\Users\Eyal\AppData\Local\Temp\fd1c28ef-8754-41b1-8f5b-cf4a953103ac.mht
Funny Birds Update #1
This program will apply update #1 to your Funny Birds product. Please connect your Funny Birds flash drive to your computer and click 'next'.
< Back
Next >
Cancel
Help

Figure 61: Sample Welcome Page

If you have included an End User License Agreement MHT file in your update, it will be displayed immediately after the welcome page. The end user must accept the license agreement in order to proceed with the update process.

This is a sample of an end user license agreement for our "Funny Birds" product.

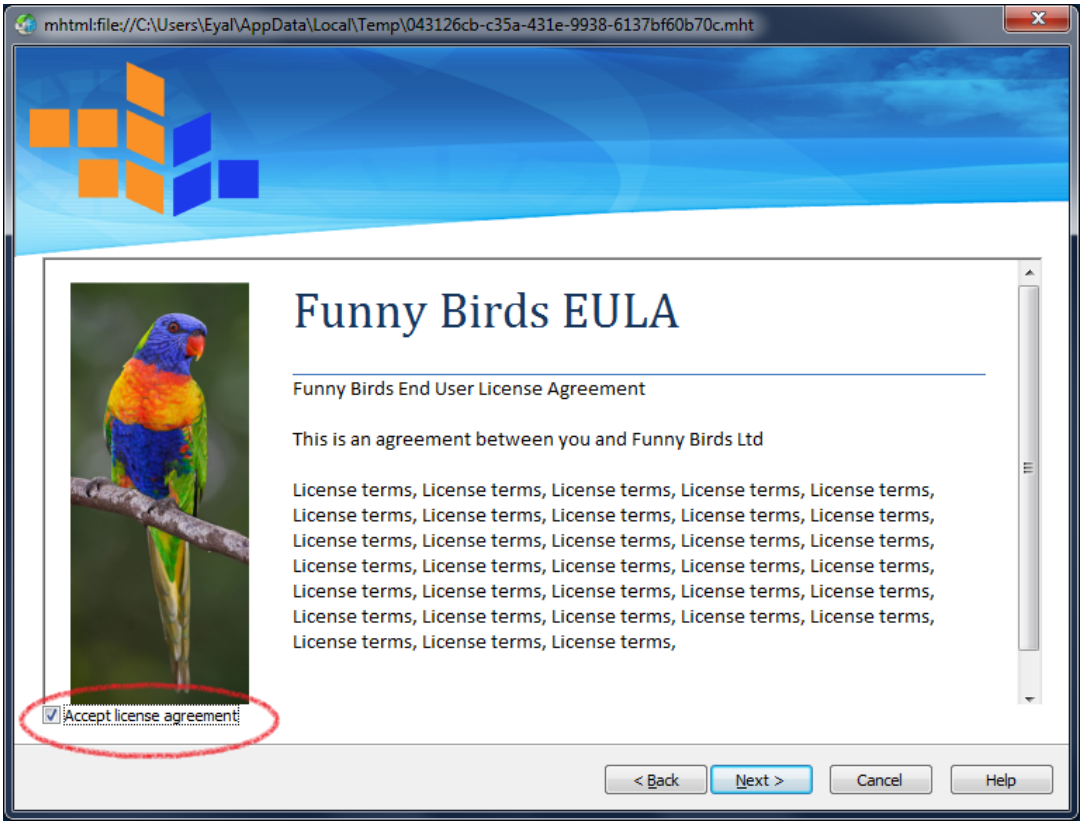
mhtml:file://C:\Users\Eyal\AppData\Local\Temp\043126cb-c35a-431e-9938-6137bf60b70c.mht
Funny Birds EULA
Funny Birds End User License Agreement
This is an agreement between you and Funny Birds Ltd
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms, License terms, License terms,
License terms, License terms, License terms,
Accept license agreement
< Back
Next >
Cancel
Help

Figure 62: End User License Agreement Sample

After the user accepts the license agreement and clicks 'Next' the software looks for compatible flash drives. The software displays a list of all TSFDs it has detected. If more than one was detected the end user can select which one he wishes to update.

On this page the end user also has to enter his license code if the update requires it. Clicking next will automatically start the update recording process.

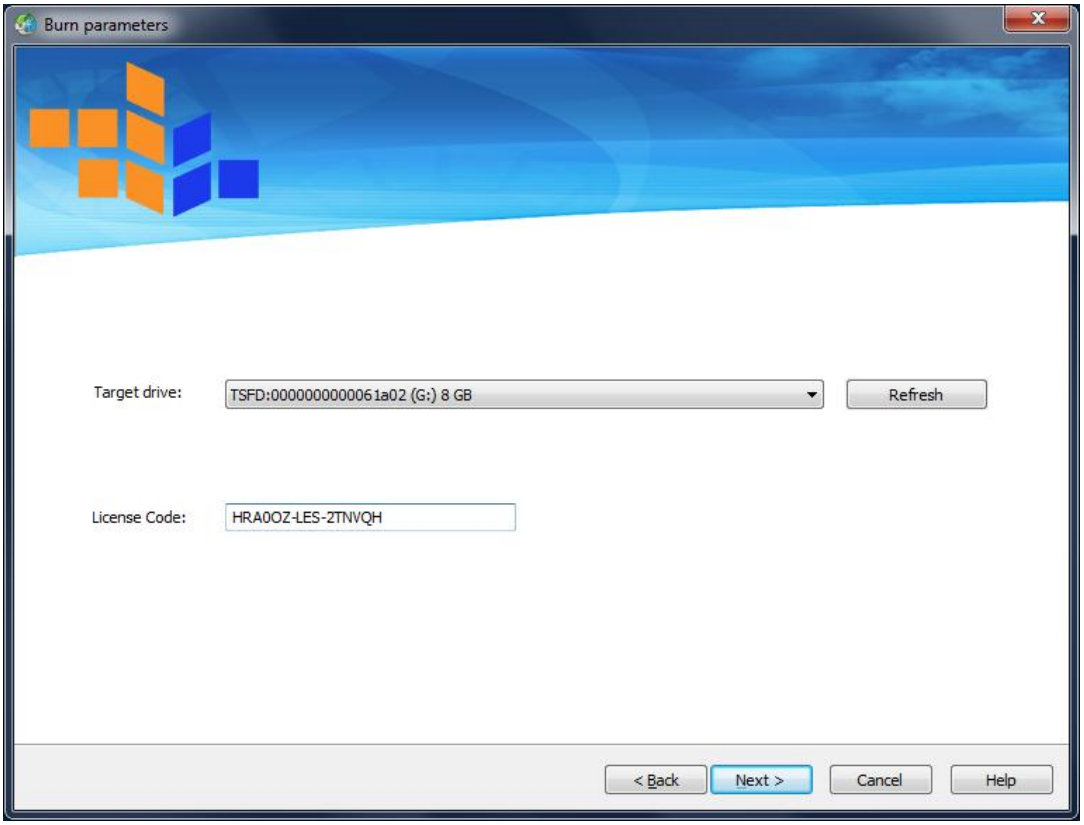

Figure 63: Target Drive and License Code

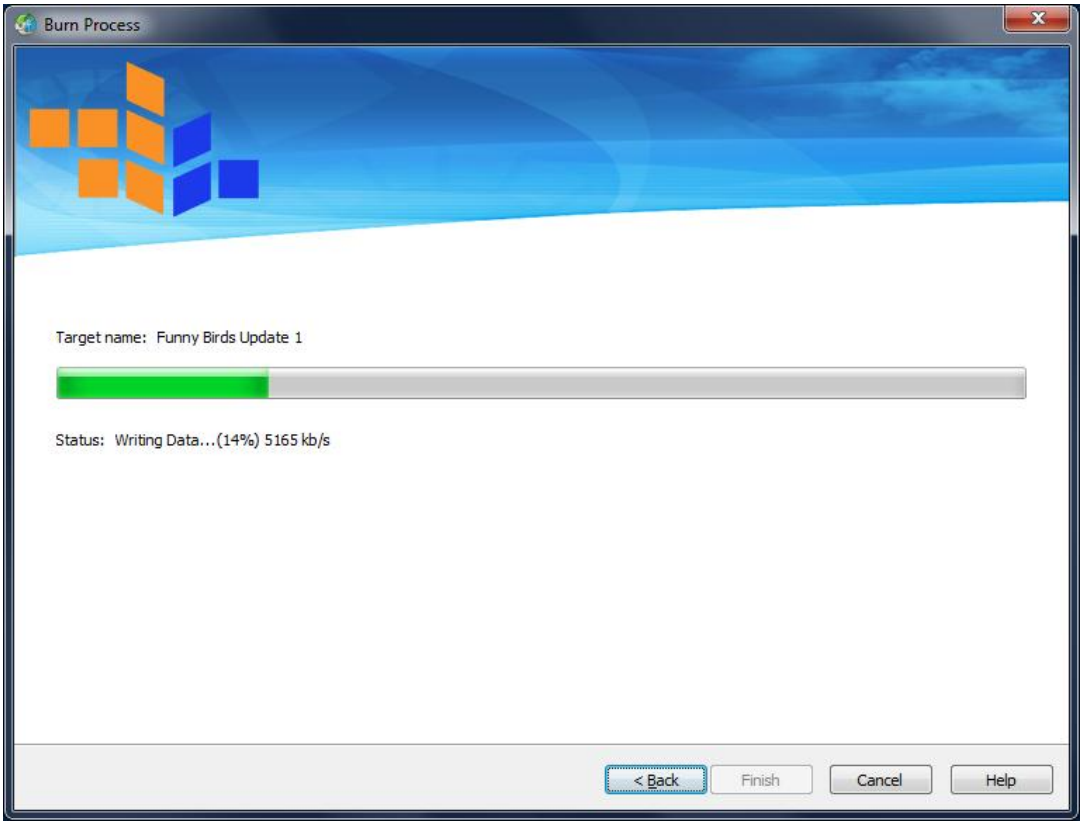

Figure 64: The Update Recording Process

9. Troubleshooting & Known Issues

A. Symptom

On the 'Edit Project' page, some files on the right panel appear with a "lock" icon and cannot be marked for protection:

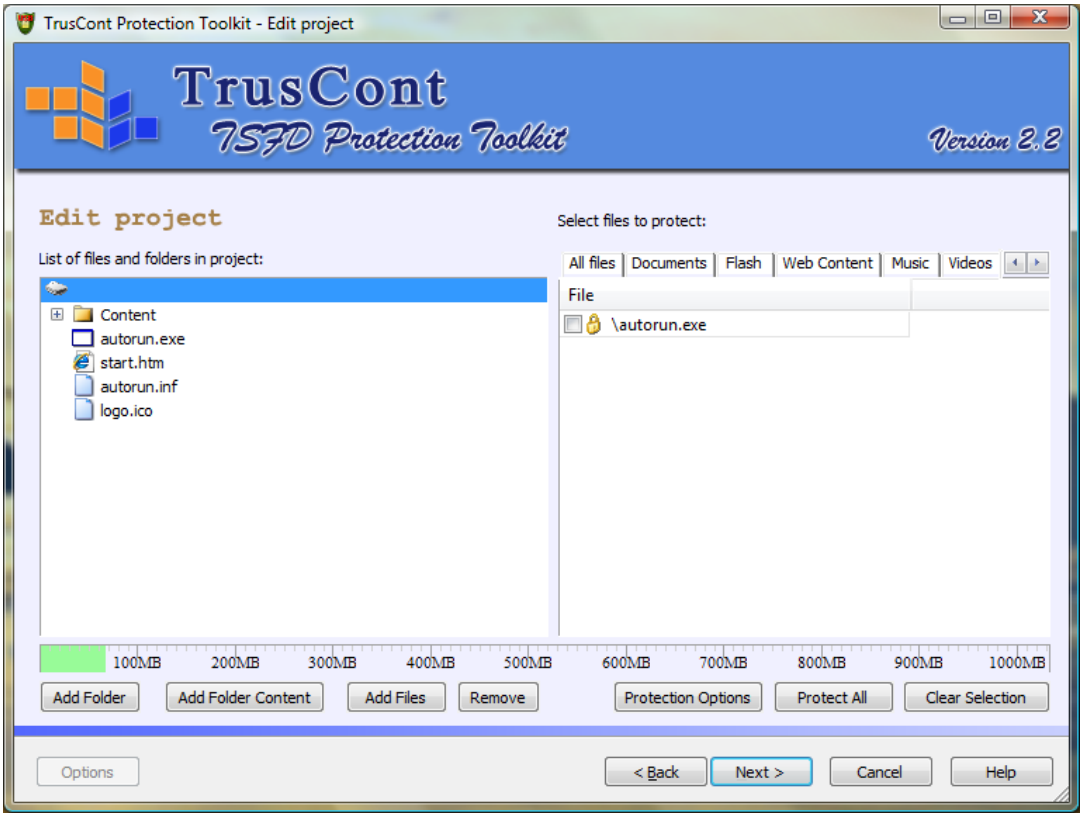

Figure 65: Previously Protected Files Indication

Resolution

The files that appear with a "lock" icon are actually files that have been protected in a previous operation. The copy protection cannot be reapplied on already protected files. Remove these files from your project and use the original unprotected copies of the files.

B. Symptom

On the 'Edit Project' page, some files on the right panel appear with a 'No-Entry' sign icon and cannot be marked for protection:

Resolution

The files that appear with a 'No-Entry' sign icon are not supported by the current version of the Toolkit. The current version supports protection of 32 bit executable files only. If the files that appear with a 'No-Entry' sign are 32 bit executables then it may have non-standard structures.

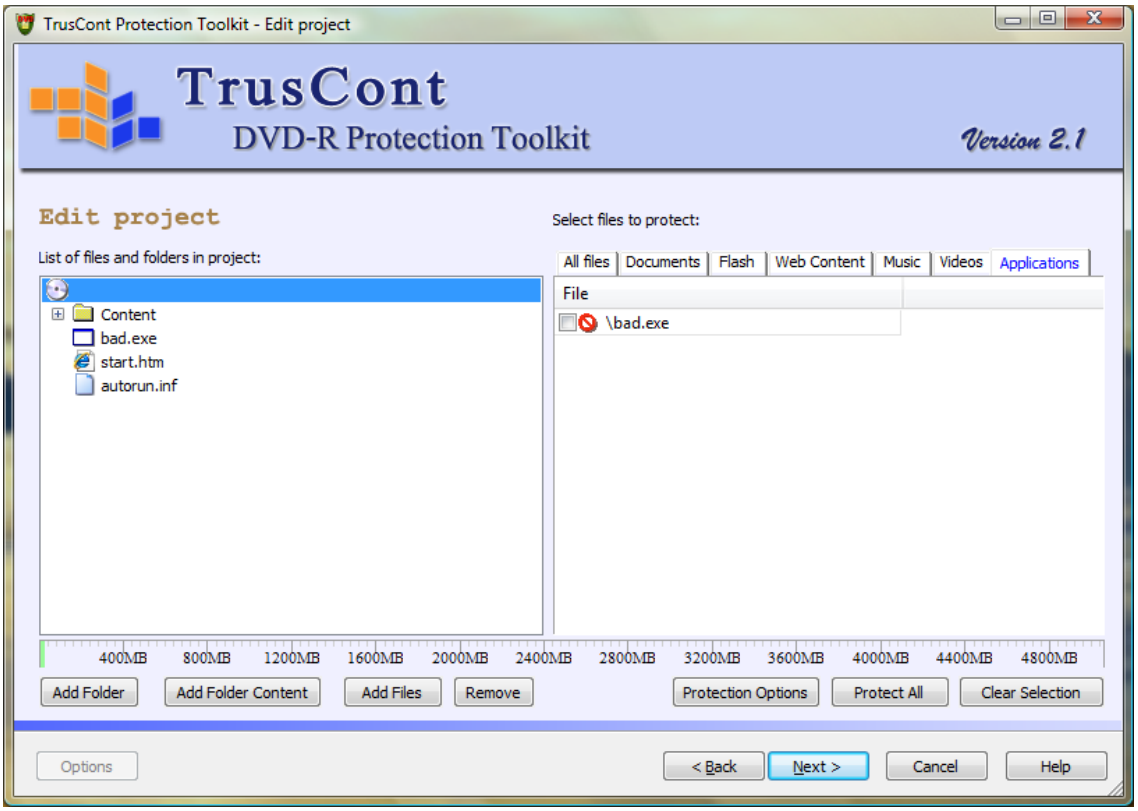

Figure 66: Unsupported Files Indication

C. Symptom

On the 'Edit Project' page, when clicking the 'Select All' button, the following message appears:

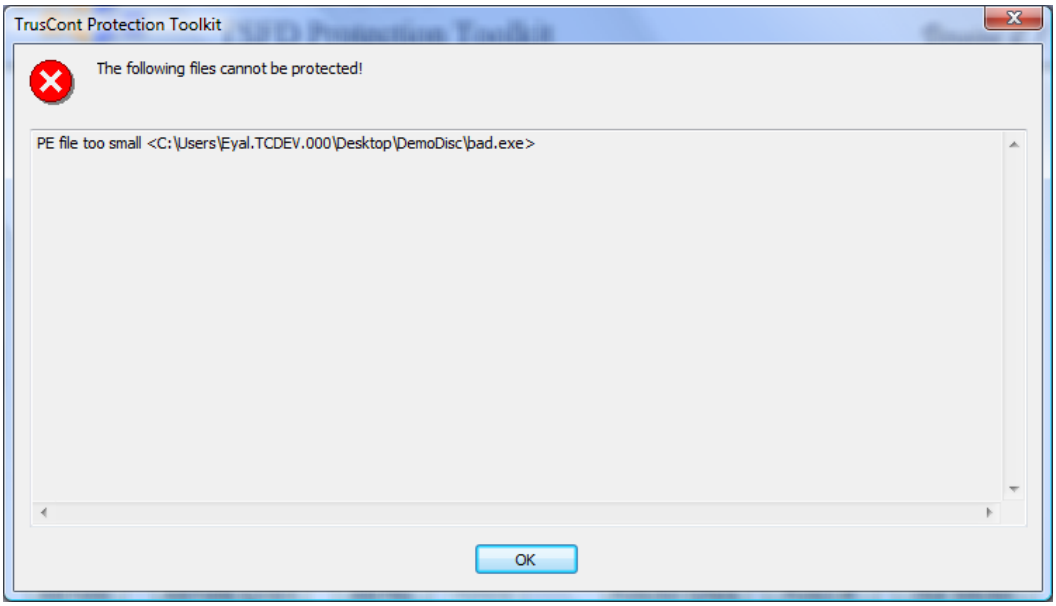

Figure 67: Unsupported Files Notification

Resolution

This message appears when you click the 'Select All' button and your project contains some executable files that cannot be protected. The message notifies you that some of the files you may wish to protect couldn't be protected.

Some files are not built strictly according to the PE file format specification (windows program files format). Some deviations from the specification may prevent the Toolkit from applying the copy protection on such files. Usually the Toolkit can detect such deviations and prevent you from marking such files for protection.

Please note that in rare occasions Toolkit may encounter such deviations only when actually trying to apply the copy protection (depending on the actual deviation). In this case you may encounter the above message just before starting the duplication process. If the problematic file(s) are not critical to protect, retry the process without protecting these files. Otherwise, please contact TrusCont support for additional assistance.

D. Symptom

When opening a saved project one of the following error messages appear:

a) Failed to open project. The file <filename> was changed.

b) Cannot open the file <filename>. The system could not find the file specified.

Resolution

When opening a saved project the Toolkit verifies the existence and integrity of the project's files. The above error messages indicate that at least one file was either changed or removed since the project was last saved. It is recommended that you reorganize your project's files, test their functionality and recreate your project using the Toolkit.

E. Symptom

When selecting a file to protect in the 'Project Edit' page the following error message appears:

"Failed to protect the file <filename>. Error: Code section too small."

Resolution

Applying the copy protection on a program file involves in injecting the copy protection software code to the program file. If the file's software code is too small this operation cannot be performed. Please note that even though the file may be very large, it may contain large resources such as graphics and text, the actual files size is usually not an indication to the file's software code size. If the specific file is critical to protect, please contact TrusCont support for further assistance.

F. Symptom

On Windows 2000 the following errors appears when connecting a TSFD with protected content files:

"RunMe.exe - Unable To Locate DLL"

"The dynamic link library FLTLIB.DLL could not be found in the specified path"

Resolution

Running protected content files on Windows 2000 requires installation of Service Pack 4 and Rollup 1. To resolve this issue download and install Microsoft Rollup 1 for Windows 2000 from the following link:

http://www.microsoft.com/downloads/details.aspx?FamilyId=B54730CF-8850-4531-B52B-BF28B324C662&displaylang=en

Appendix A – Customizing 3rd Party Applications Support for Content Protection

Introduction

By default TrusCont software allows a list of certified 3rd party applications reading protected content files. Other 3rd party (standard or proprietary) applications that are not included in this list are either not tested or not compatible with TrusCont copy protection. This appendix describes how customers can add support for additional 3rd party applications

Warning

There is no guaranty that applications not specifically certified by TrusCont and included in the default list will be able to read protected files properly. TrusCont shall not be liable for any direct and/or indirect consequences of using this feature. It is highly recommended that customers test their products thoroughly before actual publication. Testing on multiple systems and configurations is recommended in order to ensure your proprietary application can read protected files properly.

Instructions

1. Follow these instructions in order to add support for your application:
2. Open the Advanced Project Options dialog (see section *5.2.4 Changing Advanced Project Settings*) and click the 'Applications' tab.

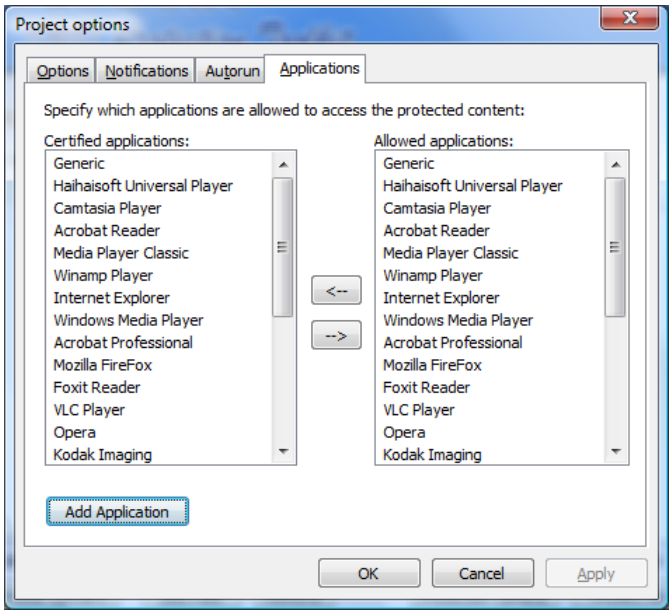

Figure 68: Certified Application List

3. Click 'Add Application'

4. Complete the application setup form according to the following guidelines:

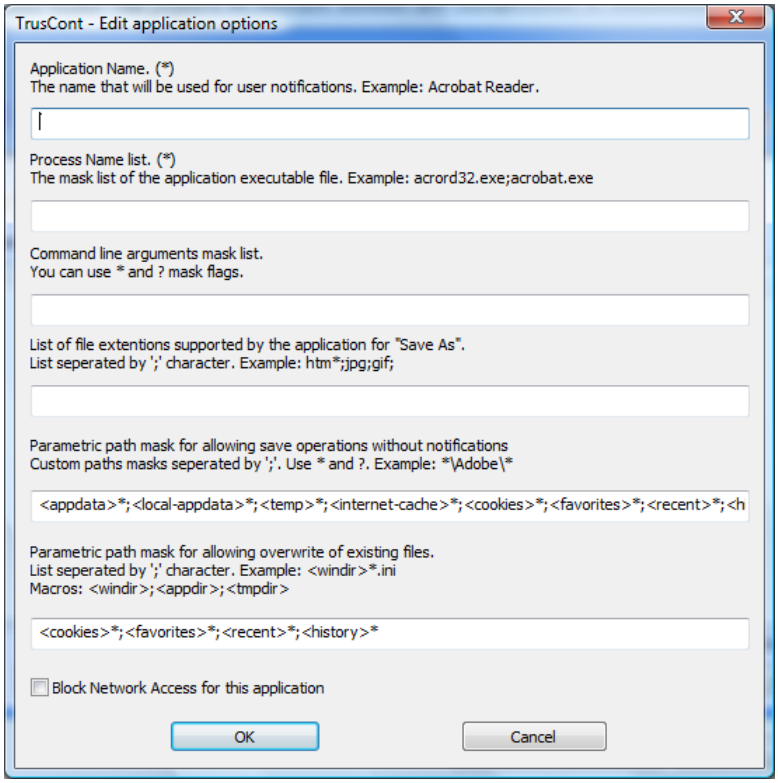

Figure 69: The Application Setup Form

a. **Application Name** – The name of your application for use in the Toolkit user interface and notifications for end users. Any text is applicable.

b. **Process Name List** – List all executable files of your application that should have access to protected content files.

c. **Command Line Arguments** – Enter command line arguments that may be required for your application.

d. **List of extensions supported by the application's "Save As" option** – List all the extension that your application typically allows to save. The Toolkit will not allow your application to save any files. However, if end users try to save files with the listed extensions from your application the Toolkit display a notification that the files cannot be saved. For all other extensions (e.g. temporary files) the Toolkit will not provide any notifications.

e. **Parametric path mask for allowing save operations without notifications** – List all paths for which the Toolkit will not display any notification even if the saved file has an extension included in the list of the previous section (d).

f. **Parametric path mask for allowing overwrite of existing files** – List all paths for which the Toolkit will allow overwriting of existing files. By default the copy protection doesn't allow overwriting of protected files because all writes are encrypted. Overwriting existing files with encrypted data makes the files invalid. You should include in this path list only locations that do not contain important files that your application may overwrite.

g. **Block network access for this application** – Specify whether or not you wish your application to have network access when reading protected files. Block network access if you suspect that your application may allow transmission of data read from protected files through a network.

Appendix B – TSFD License Requirements by Features

TrusCont offers 2 different TSFD Models – TSFD Publisher, and TSFD Ready. The table below lists the features included with the built-in license of each model. Features not included within the built-in license require a license upgrade which can be purchased from TrusCont representatives worldwide.

Feature	TSFD Ready	TSFD Publisher
Read-Only Partition	✓	✓
CD-ROM Partition	✓	✓
Multi-partition support	✓	✓
Autorun & Autoplay support	✓	✓
Bootable	✓	✓
Rewriting RO/CDROM partitions	License upgrade required [1]	✓
Anti-Copy for software	License upgrade required [2]	✓
Anti-copy for content files	License upgrade required [2]	✓
Control printing and Copy & Paste	License upgrade required [2]	✓
Access Control	License upgrade required [2]	✓
Time-Limit protection	License upgrade required [2]	✓
Internet Updates	License upgrade required [2]	✓
Limit number of Installations	License upgrade required [2,3]	License upgrade required [3]
Limit use to specific # of users/computers/domains	License upgrade required [2,3]	License upgrade required [3]
Internet Publishing (USB)	License upgrade required [2,4]	License upgrade required [4]

Notes:

1. Each TSFD Ready flash drive includes a license for one write of a CD-ROM or Read-Only partition. Additional rewrites require a "Read-Only USB License" for each rewrite.
2. Copy protection features require an upgrade to TSFD Publisher – one TSFD Publisher License for each flash drive.
3. Requires the Lock to User/Computer/Domain license – one license for each user/computer/domain/installation.
4. Requires a "Publish to USB" license for each copy of the data published to a TSFD Publisher

Appendix C – The TSFD License Term

TSFDs come with a 1 year, unlimited overwrites license. This means you can overwrite or update the protected content of your TSFDs unlimited times during 1 year.

There are 2 basic methods for updating a TSFD:

1. Overwrite a TSFD using the TSFD Protection Toolkit. This is method requires physical access to the TSFD you wish to update.
2. Create an update file for TSFDs. The update file is an EXE that contains the updated content. It automatically installs itself to the target TSFD similar to a program setup file. This method is useful for updating TSFDs that were already sent to customers. The update file can be downloaded, or delivered on physical media.

What happens when the 1 year license expires?

After the 1 year license expires the protected content on the TSFD remains readable but cannot be overwritten unless you renew the TSFD license. Of course your content remains protected. If the TSFD has a second read-write partition your customer may continue using the second partition as a standard removable drive – just like before the license has expired.

Renewing a TSFD License

There are 2 basic methods for renewing the license of TSFDs:

1. Overwrite a TSFD using the TSFD Protection Toolkit

   You can renew the license at the same time you overwrite the TSFD with new content. If the TSFD license has expired the TSFD Protection Toolkit will ask you for your TrusCont username (email) and password. The Toolkit will then pool 1 TSFD license from your TrusCont account. Check your TrusCont Account Balance to make sure you have at least one TSFD license. Contact your TrusCont representative to obtain additional TSFD licenses.

2. Create a License Code

   Sometimes content owners wish to update TSFDs that were already sent to customers. This is done by sending the customers an update file. If the license of a customer's TSFD has expired the update file will ask the customer for a license code. Create a license code with one TSFD Publisher license (in addition to other licenses required for the update) and send it to your customer. See section *8.3.3.3, Generating License Code for End Users*, for further instructions.

Appendix D – TrusCont Content Publishing Server

TrusCont Content Publishing Server is the world's first all-in-one content publishing system.

The TCPS is by far the most advanced powerful and comprehensive publishing equipment your money can buy. Everything you will ever need packed in a simple, easy to use interface, and high end hardware optimized and fine-tuned for the best performance and efficiency.

Figure 70: TrusCont Content Publishing Server

Features:

- High-end hardware
- **Windows 7** Operating System
- Fully Supports **TrusCont Secure Flash Drives**, and **TrusCont Enhanced DVD-R**.
- Duplicates **CD/DVD/USB/MicroSD**.
- Extendable – So powerful it **can drive also external devices** and hubs you attach to it.
- **Integrated File Repository** and File Server – allows customers to upload files to the server
- **Duplicate Multiple Jobs at the Same Time** – jobs are automatically routed to the next available device
- **Job Queuing** – queue multiple jobs, the server will start them automatically according to their position in the queue.
- **Remote administration** – manage your server, and production from anywhere in the world via the Internet.
- **On Demand** features – allow your customers to master their content and upload it for duplication.
- Powerful Anti-Copy & DRM Features

Visit the TCPS web page for additional info: http://www.truscont.com/?page=38&id=78

Additional Support Information

TrusCont Support Center: http://support.truscont.com
Email support: support@truscont.com
Phone: +972 4 832 0555 (English, Russian, Hebrew 9am – 6pm GMT +2)
Fax: +972 4 832 0550

TrusCont Ltd
87 Moshe Goshen Ave., Qiryat Motzkin 26313, Israel

For support in your language and local business hours please locate the nearest representative to your location on our Contact Us page at http://www.truscont.com/?page=3